Report on Member States' Progress in Implementing the EU Toolbox on 5G Cybersecurity

July 2020

NIS COOPERATION GROUP

Report on Member States' progress in implementing the EU Toolbox on 5G Cybersecurity

Table of Contents

Introduction

1.1. Background

In March 2019, the **EU the Heads of State or Governments** called for a concerted approach to the security of 5G networks. Following this, the European Commission adopted the **Commission Recommendation on the Cybersecurity of 5G networks**[1] ('The Recommendation'), which set out a number of concrete actions at national and Union level to strengthen the cybersecurity of 5G networks.

First of all, each Member State completed a national risk assessment of its 5G network infrastructures and transmitted the results to the Commission and ENISA, the European Union Agency for Cybersecurity, by early July 2019. Based on these national risk assessments, on 9 October 2019 the NIS Cooperation Group, formed of representatives of Member States, the Commission and ENISA, published a report on the **EU Coordinated Risk Assessment on Cybersecurity in 5G Networks**[2]. The report identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities (including technical ones and other types of vulnerabilities) affecting 5G networks. On this basis, the report also identified a number of categories of risks of strategic importance from an EU perspective illustrated by concrete risk scenarios, which reflect relevant combinations of the different parameters (vulnerabilities, threats and threat actors) with respect to the different assets.

To complement this report, ENISA carried out a dedicated **threat landscape mapping**, consisting of a detailed analysis of certain technical aspects, in particular the identification of network assets and of threats affecting these.

On 29 January 2020, the NIS Cooperation Group published the **EU toolbox of risk mitigating measures**[3] **('the Toolbox')**. It addresses all the risks identified in the EU coordinated risk assessment report. On the same date, the Commission adopted a **Communication (Secure 5G deployment in the EU - Implementing the EU toolbox)**[4]**,** in which it endorsed the measures outlined in the Toolbox conclusions and underlined the importance of their effective and quick implementation and called on Member States to take concrete first steps to implement them by 30 April 2020 and to prepare a report on their implementation by 30 June 2020.

In its Conclusions of 9 June 2020[5], the Council '*recognises that increased connectivity, while empowering digital services, can result in citizens, companies and governments being exposed to cyber threats and crimes that are increasing in number and sophistication*. In this context, it '*emphasises the importance of safeguarding the integrity, security and resilience of critical infrastructures, electronic communications networks, services and terminal equipment*' and '*supports the need to ensure and implement a coordinated approach to mitigate the main risks, such as the ongoing joint work based on the EU toolbox on 5G cybersecurity and the secure 5G deployment in the EU*.'

[1] Commission Recommendation (EU) 2019/534 on the Cybersecurity of 5G networks, 26 March 2019

[2] https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

[3] https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

[4] Commission Communication COM (2020)50, Secure 5G deployment in the EU - Implementing the EU toolbox, 29 January 2020.

[5] Council Conclusions on Shaping Europe's Digital Future, 9 June 2020.

Moreover, the central importance of digital connectivity has been made even more prominent during the Covid-19 crisis, underlining the considerable existing reliance of our societies on telecommunications networks and digital infrastructures and services, and therefore the importance to promote the roll-out of 5G networks in a way that is both swift and secure.

In terms of 5G deployment, at the end of May 2020, 5G commercial services had been deployed in 12 Member States: Austria (3 operators with 5G commercial service), Belgium (1), Finland (3), Germany (2), Hungary (1), Ireland(2), Italy(2), Latvia (3), The Netherlands (1), Romania (3), Spain(1) and Sweden (3). In what concerns the promotion of early deployment in major urban areas and along major transport paths, 191 trials were reported[6]. During the coming few months, it is foreseen that 5G spectrum assignments will take place in several EU Member States, thus enabling their operators to launch commercial 5G services.

As regards network security, mobile operators are currently subject to a supervisory system under the EU Telecommunications Framework aimed at verifying the effective implementation of security policies, as well as the notification of significant incidents. A majority of Member States currently have basic security obligations in place, based on the current EU Telecommunications Framework and some have imposed detailed requirements, mostly of technical nature. Building on this baseline, the Toolbox recommends that additional security measures are introduced to specify detailed obligations for 5G networks, addressing a range of identified risks and taking into account both technical and non-technical factors. Specifically, the Toolbox identifies and describes a set of **Strategic and Technical measures**, as well as corresponding supporting actions to reinforce their effectiveness, which may be put in place in order to mitigate the identified risks.

Strategic measures cover measures concerning increased regulatory powers for authorities to scrutinise network procurement and deployment, specific measures to address risks related to non-technical vulnerabilities, as well as possible initiatives to promote a sustainable and diverse 5G supply and value chain in order to avoid systemic, long-term dependency risks. **Technical measures** include measures to strengthen the security of 5G networks and equipment by addressing the risks arising from technologies, processes, human and physical factors. Moreover, for each of the risk areas identified in the EU coordinated risk assessment, the Toolbox provides for **risk mitigation plans** based on the **highest effectiveness measures**. Based on the assessment of possible mitigation plans and the identification of highest effectiveness measures, the Toolbox recommends that **all Member States should take a number of actions, which are set out in the conclusions of the Toolbox report.**

1.2. Objectives and content of the report

This document constitutes the report on the implementation of the Toolbox referred to in the Commission Communication. Its main objective is to provide an overview of the state of play of the ongoing Toolbox implementation process by Member States as of June 2020. It was prepared and agreed by the NIS Cooperation Group, with the support of the Commission and ENISA.

The Toolbox includes measures to be taken at national and at EU level. This report focusses on the steps to be taken by Member States at national level. Aside from what is presented in this report, there are additional ongoing strands of work at EU level, such as the actions initiated on 5G standardisation and certification or policies under preparation by the Commission to support EU capacities and a sustainable 5G value chain in the EU.

[6] Source: 5G Observatory and public announcements by mobile operators.

The report provides a factual analysis of the steps taken by Member States to implement the Toolbox since it was published on 29 January 2020.

Specifically, based on the information gathered, and bearing in mind certain limitations detailed below, the report provides:

- The current status of implementation of key toolbox measures;
- The nature of the national measures adopted or planned, where information has been made available;
- An initial assessment of the degree of convergence of adopted and planned measures;
- An initial assessment of possible gaps and areas where further action is needed.

This report is also intended to inform on the future steps in the EU coordination process on 5G cybersecurity, including the assessment of the effects of The Recommendation.

1.3. Methodology

The results of this report are based on information provided by Member States in the framework of the NIS Cooperation Group Work Stream on 5G Cybersecurity. This information was gathered between 15 May and end of June, notably through a standardised template to which 26 Member States provided answers, and through further inputs and discussions during Work Stream meetings. The report also refers to relevant findings of an internal survey concluded by BEREC in November 2019 as an input to the EU coordinated process on 5G cybersecurity.

National implementation processes are ongoing and, despite the challenging circumstances related to the Covid-19 crisis, possible substantial delays in the implementation process have been communicated by very few Member States only. However, in many Member States, the draft measures are either still being discussed or consulted or are awaiting a political decisions. In addition, in certain cases, for other reasons (absence of political decision or insufficient information provided), the lack of information available at the time of writing this report limited the analysis that can be made on susbtance. Moreover, some Member States in which the implementation process is already well-advanced or where measures have been already adopted, did not share detailed information on individual measures for the purpose of this report (in some cases for national security reasons).

For each of the Toolbox measures the report also gives an indicative implementation maturity level, roughly illustrating how far, on average, Member States are advanced with their implementation of respective measures. These indicative levels are determined based on an ad-hoc methodology that takes in consideration several factors, namely declared current implementation status, declared planned dates of completion and estimated levels of completeness of the data provided by Member States.

Implementation maturity ➔ Toolbox measure ➔	Very Low	Low	Low-Medium	Medium	Medium-High	High	Very High
SM01: Strengthening the role of national authorities					●		
SM02: Performing audits on operators and requiring information				●			
SM03: Assessing the risk profile of suppliers and applying restrictions[7] for suppliers considered to be high risk				●			
SM04: Controlling the use of Managed Service Providers (MSPs) and equipment suppliers' third line support				●			
SM05: Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies		●					
SM06: Strengthening the resilience at national level		●					
SM07: Identifying key assets and fostering a diverse and sustainable 5G ecosystem in the EU			●				
TM01: Ensuring the application of baseline security requirements (secure network design and architecture)					●		
TM02: Ensuring and evaluating the implementation of security measures in existing 5G standards			●				
TM03: Ensuring strict access controls					●		
TM04: Increasing the security of virtualised network functions			●				
TM05: Ensuring secure 5G network management, operation and monitoring				●			
TM06: Reinforcing physical security				●			
TM07: Reinforcing software integrity, update and patch management				●			
TM08: Raising the security standards in suppliers' processes through robust procurement conditions			●				
TM11: Reinforcing resilience and continuity plans					●		

Table 1: Overview of the level of maturity in the implementation of the Toolbox measures

[7] Including necessary exclusions to effectively mitigate risks- for key assets.

2. Member States' progress in implementing the Toolbox measures

As stated above, the Toolbox identifies a possible common set of measures which are able to mitigate the main cybersecurity risks of 5G networks, and provides guidance for the selection of measures which should be prioritised in mitigation plans at national and at Union level.

The **highest effectiveness measures** identified in the Toolbox conclusions and recommended for implementation by all Member States at national level cover:

- Strengthening the **role and powers of regulatory authorities** (Strategic measures 01 and 02);
- Assessing the risk profile of suppliers; as a consequence, **applying relevant restrictions for suppliers considered to be high risk - including necessary exclusions to effectively mitigate risks - for key assets** defined as critical and sensitive in the EU coordinated risk assessment (e.g. core network functions, network management and orchestration functions, and access network functions) (Strategic measures 03 and 04);
- Ensuring that each operator has an appropriate multi-vendor strategy to **avoid or limit any major dependency** on a single supplier (or suppliers with a similar risk profile), ensure an adequate balance of suppliers at national level and **avoid dependency on suppliers considered to be high risk** (Strategic measures 05 and 06);
- Maintaining a diverse and sustainable 5G supply chain in order to avoid long-term dependency, including by: making full use of the existing EU tools and instruments. (Strategic measures 07). ***N.B: This report covers national FDI frameworks only;***
- Strengthening **security requirements on operators** (Technical measures 01 to 08 and 11).

In addition, other actions have been launched or will be taken at EU level to support the objectives of Strategic Measures 07 and 08, as announced in the Commission Communication of 29 January. These include action aimed at further strengthening **EU capacities in the 5G and post-5G technologies**, by using relevant EU programmes and funding. Moreover, Member States, with the support of the Commission and ENISA, have taken first steps to facilitate coordination between Member states regarding **standardisation** to achieve specific security objectives **and to develop relevant EU-wide certification scheme(s)** in order to promote more secure products and processes.

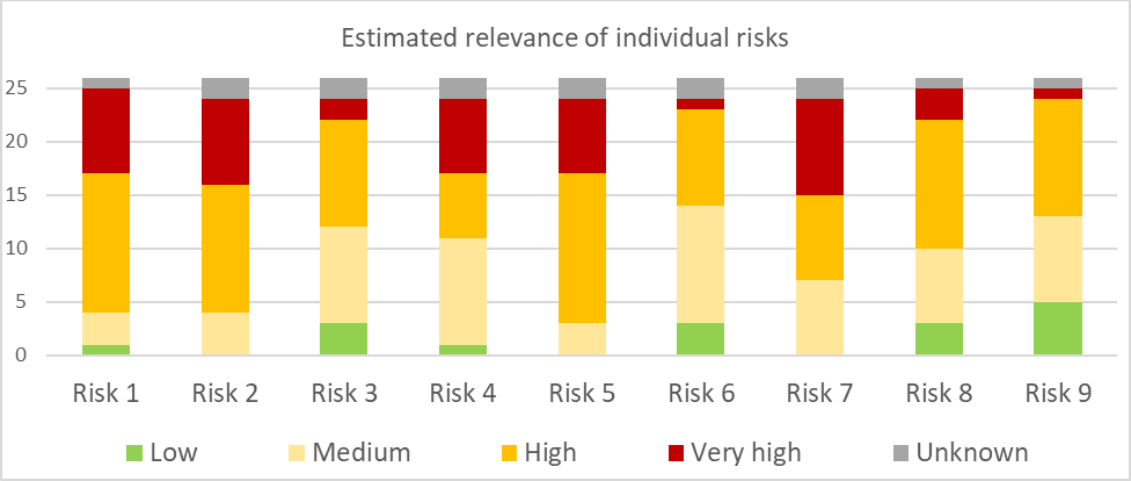
As outlined in the Toolbox, Member States will need to take a range of mitigation actions to effectively address the risk posed by 5G. In order to determine appropriate mitigation actions, Member States are also advised to consider prioritising risks according to the national/EU Coordinated Risk Assessment and reviewing the effectiveness of existing mitigations in addressing the risks in the Risk Assessment, including identification of gaps[8].

Based on the input provided in response to the questionnaire related to **relevance of risks**, illustrated on the chart below, it can be concluded that the top three relevant risks highlighted by Member States are:

- *R1-Misconfiguration of networks* (considered as high or very high by 21 Member States)

[8] Toolbox section 5.2, Table 4, steps 1 and 1a.

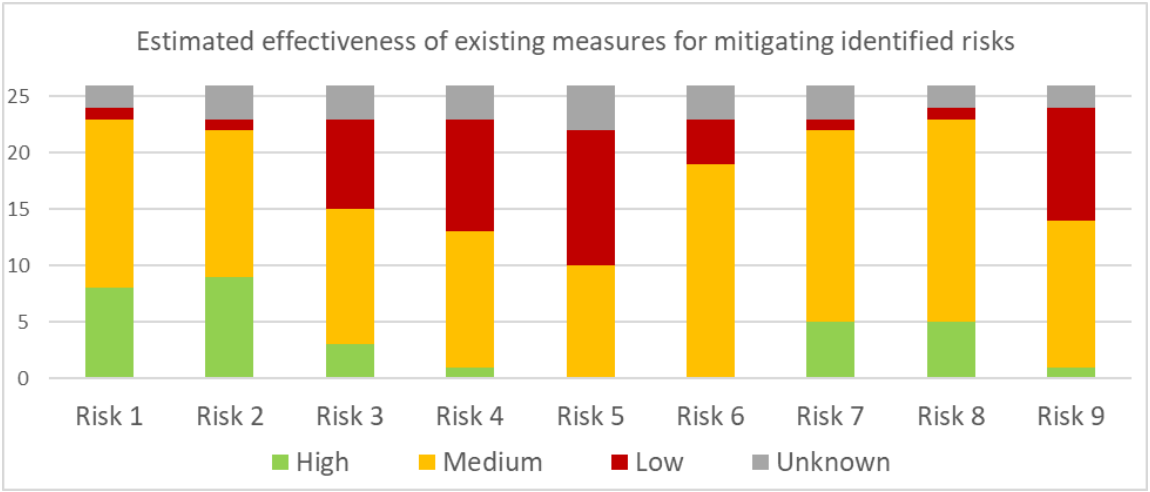
- *R2-Lack of access controls* (considered as high or very high by 20 Member States)
- *R5-State interference through 5G supply chain* (considered as high or very high by 21 Member States)



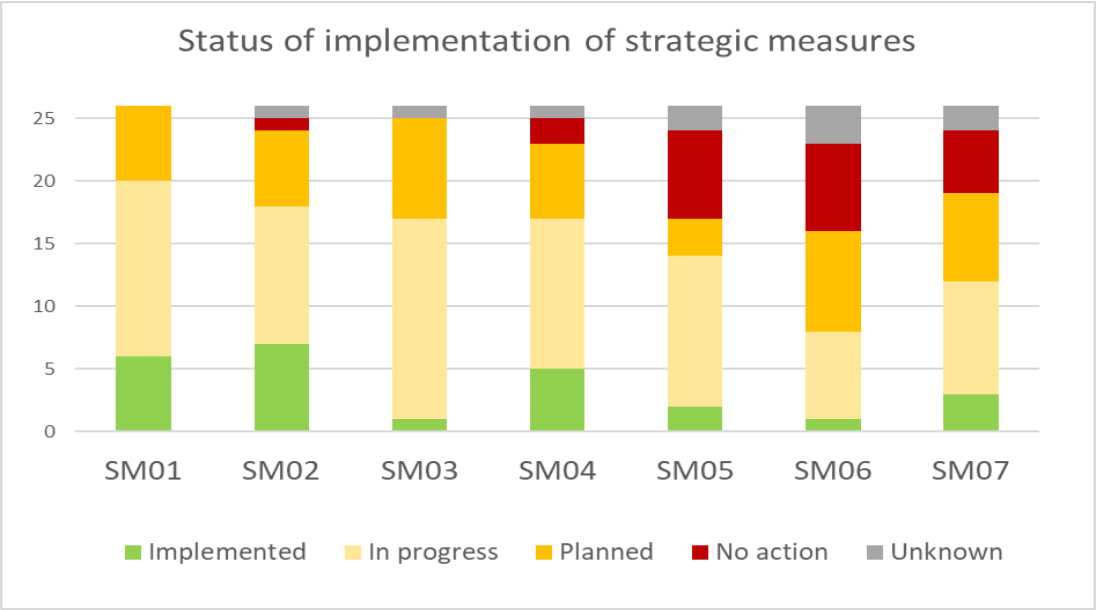
On the other hand, the input related to **effectiveness of existing measures in mitigating identified risk**, illustrated on the chart below, highlights several risks that appear to be mitigated to the lowest extent with existing measures:

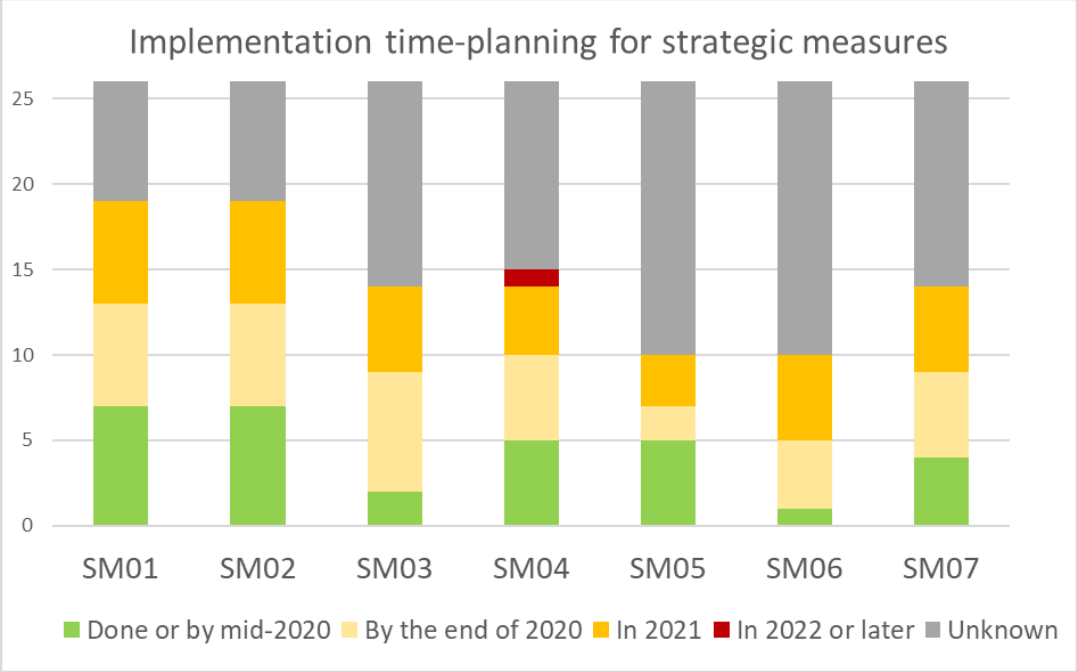
- *R4-Dependency on any single supplier within individual networks or lack of diversity on nation-wide basis* (only 1 Member State considers existing measures to be highly effective)
- *R5-State interference through 5G supply chain* (no Member State considers existing measures to be highly effective)
- *R6-Exploitation of 5G networks by organised crime or organised crime group targeting end-users* (no Member State considers existing measures to be highly effective)
- *R9-Exploitation of IoT* (Internet of Things), handsets or smart devices (only 1 Member State considers existing measures to be highly effective)

Correlation of the two findings explained above highlights in particular the risk R5 (State interference through 5G supply chain) as being both the most relevant and least mitigated.



2.1 Implementation of Strategic measures





A large number of Member States have already taken concrete steps to implement the various Strategic Measures. At the same time, however, there are visible differences in terms of implementation maturity for different types of individual measures. In the next sections we present more details and specific findings from the assessment of each of the Strategic Measures, based on the data provided by Member States.

2.1.1 SM01 - Strengthening the role and powers of regulatory authorities

This should include regulatory powers for national authorities, to be able to:

- impose strengthened obligations on operators, for example concerning the security of the signalling/management plane;

- use ex-ante powers to restrict, prohibit and/or impose specific requirements or conditions, following a risk-based approach, for the supply, deployment and operation of the 5G network equipment, taking into account among other things:

- Security of critical and sensitive parts of 5G networks;

- Security of the equipment itself or the environment (deployment, interconnections, etc.);

- Risk of interference by a third country in the 5G supply chain;

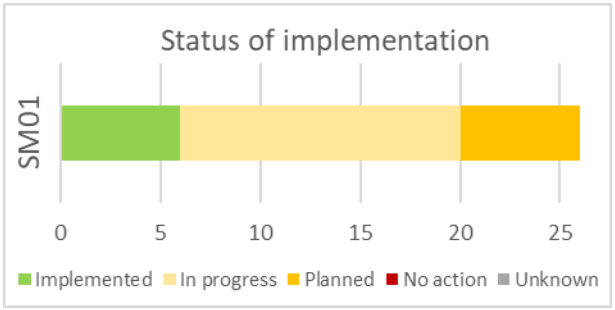
- Risk of major dependency on a single supplier by individual MNOs or nationally

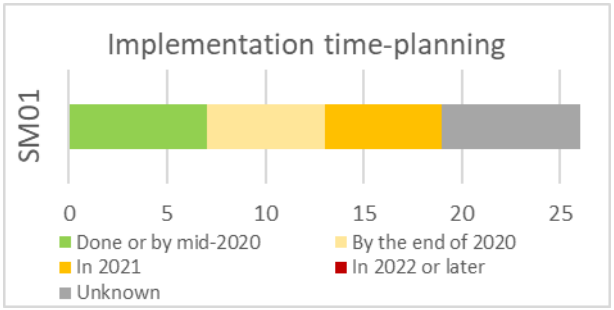
- Risks for national security.

Status of implementation – statistics

The data submitted by Member States shows a **MEDIUM to HIGH** level maturity for this measure. In a large majority of Member States, measures aimed at strengthening the role of national authorities are either already implemented or in progress. In many of those Member States, the measures are expected to be finalised by the end of the year. For the remaining Member States, measures are planned for 2021.

More specifically, six Member States have already adopted measures while this is in progress in fourteen Member States (in eight of them the preparation of measures is already well advanced). A third group of Member States are planning to take measures or have launched preparatory work. Among this last group, four Member States have not communicated clear plans or are still considering whether or not specific action will be taken.





Status of implementation – details

Reinforcing the powers of national authorities in order to ensure the cybersecurity of 5G networks is considered in the Toolbox both as a prioritised measure that all Member States should put in place as well as a pre-requisite for ensuring the applicability and the effectiveness of the other Toolbox measures. It is being implemented by Member States as part of or as a complement to the transposition of the European Electronic Communications Code.

A significant number of Member States have now introduced or have communicated detailed plans to introduce a legal basis to be able to impose restrictions or to prohibit the supply, deployment and

operation of 5G network equipment, whereas until now they only had had ex-post powers and controls and/or no powers to regulate the procurement of equipment and services by operators.

Among them, several Member States have or are considering putting in place of a pre-authorisation or notification mechanism[9], allowing them to assess operators' 5G deployment plans on a case-by-case basis, by requiring operators to either seek approval before deploying 5G equipment or to notify their plans to authorities who can in certain cases mandate specific restrictions or prohibitions. In these Member States, this mechanism will also enable other Strategic measures related to supply chain risks (in particular Strategic measure 03 and Strategic measure 04 and in some cases also Strategic measures 05 and 06). Through these mechanisms, authorities may indeed be able to impose additional security requirements tailored to particular deployment plans, to restrict the use of specific suppliers based on their risk profile or to limit or avoid dependencies on suppliers.

Other Member States have proposed or are considering measures to grant authorities the powers to order the removal of equipment in case they are suspected of being a threat to national security.

For all these measures, there are similarities in the methodology followed for the screening of the operators' plans or existing equipment. For instance, in all cases, assessments are taking into account both technical and non-technical factors (e.g. such as the origin of the suppliers and/or the risk of interference by a third country). Moreover, decisions based on such mechanisms may also in some Member States apply retroactively, i.e. to existing equipment used in legacy parts of the networks. In terms of implementation, most Member States have adopted specific legislation to introduce these mechanisms. In addition, to date, two Member States have adopted the approach of including these requirements into security related provisions attached with the rights of use for new spectrum assignments while three Member States are considering doing so.

Other relevant findings

Main implementation factors and considerations raised in relation to the implementation of these measures include the need to dedicate adequate resources to regulatory authorities and, when it comes to assessing and authorising the deployment of 5G equipment, the relevance of sector-specific costs, which will depend on the degree of intervention and potential impact on contractual relationships. Another aspect that is subject to ongoing reflections is how to define the exact scope of the powers and measures and whether to apply them also to new types of MNOs, such as smaller closed 5G networks serving critical functions, for example a harbour or a hospital.

Illustrative examples

Estonia 	*The Estonian Parliament approved an amendment to the Electronic Communications Act, which gave the government the power to impose obligations on communications undertakings to provide information on the hardware and software used in the communications network, and to apply for an authorisation for the use of communications network hardware and software in order to guarantee national*

[9] According to the BEREC internal survey, in November last year, such legislation was in place in only one Member State.

		security. These obligations will be imposed and procedure will be regulated in secondary legislation.
France		*The Law N 2019-810 of 1st August 2019 provides authorities with the necessary power to restrict or prohibit or impose requirements or conditions for the supply, deployment and operation of 5G equipment by making it mandatory to get an authorisation from the Prime Minister before rolling-out and operating sensitive equipment for 5G (and future technology, e.g. 6G) networks.*
Sweden		*Through a change to the Electronic Communications Act, a condition is added that Permission to 'use radio transmitters' can only be approved if 'it is considered that radio usage will not cause harm to national security'. Spectrum auctions for 5G frequencies are having conditions attached for the actors that wish to apply to bid for the frequencies. The method of evaluation is still under discussion with the relevant actors and authorities.*

2.1.2 SM02 - Performing audits on operators and requiring information

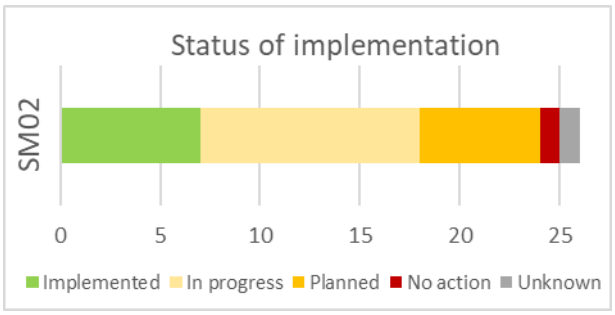
In exercising their powers under Article 41(2) of the EECC, competent authorities should:

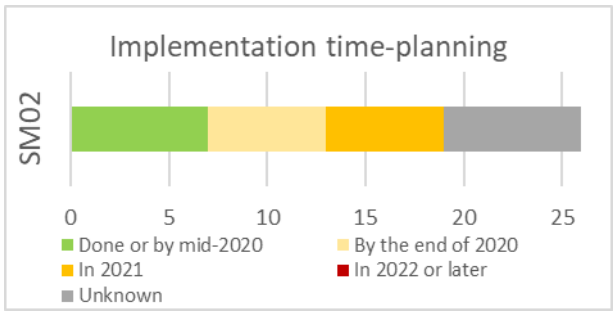
- *Audit, or require audits, of MNOs, if needed at an in-depth technical level, for example of critical components and/or sensitive parts of the 5G networks;*
- *Require operators to provide detailed and up-to-date information about their plans for the sourcing of 5G equipment and for the involvement of third party suppliers;*
- *Require operators to document and maintain a description on how the baseline technical network security measures are implemented.*

This Strategic measure aims, on the one hand, at increasing the use of existing powers to carry out security audits and to perform them in a more in-depth way, and on the other hand, at ensuring that regulators have the right information to be able to monitor the implementation by MNOs of imposed security obligations. It is therefore an important corollary of Strategic measure 01 (regulatory powers) and is necessary to ensure the effective implementation, monitoring and enforcement of the other Toolbox measures. In particular, imposing effective measures related to the use of specific suppliers requires national regulators to be informed about the current degree of involvement of the various third party suppliers in existing networks and to receive appropriate information ahead of future deployment plans.

Status of implementation – statistics

The information provided by Member States shows that this measure is currently at a **MEDIUM** level of maturity. Its implementation is considered as completed or in progress in a majority of Member States. A small minority have not provided information or indicated plans in this area. Where the process is ongoing, it is expected to be concluded in 2020 by seven Member States while in six Member States this will be the case in 2021. In the remaining Member States, no timeframe has been provided.





Status of implementation – details

Looking at the detailed answers provided by Member States, the maturity level indicated above refers to the fact that responsible authorities are empowered to conduct security audits of networks under existing EU and national telecoms rules, either autonomously or by delegating them to accredited bodies, as concluded in a BEREC internal survey[10]. According to the same survey, in a majority of Member States, audits based on existing telecoms security requirements have been performed in the last 3 years. However, this has not been the case in a significant number of Member States.

When it comes to assessing whether the objective of SM02 are being met (performing in-depth audits and requiring certain information from operators), most Member States have not provided sufficiently detailed information in order to analyse these aspects, i.e. whether they are planning to perform more regular and detailed audits and to request more information from operators as per SM02.

Based on available information, as regards information requirements, those Member States who have adopted or are preparing legislation imposing a pre-authorisation or notification system for the deployment of 5G equipment (SM01) indicated that through this mechanism, operators will be obliged to communicate detailed information to authorities about security measures and about the sourcing of 5G equipment and involvement of third party suppliers as part of their notification with a view to obtaining an authorisation, thus fulfilling at least part of the objective of SM02.

As far as audits are concerned, the BEREC survey showed that as of last year there were no national audit methodology in place in most Member States. In relation to the toolbox implementation, only two Member States have announced plans to develop a more detailed audit and compliance monitoring framework for 5G networks and one Member State indicated that enhanced transparency requirements concerning the relations between operators and suppliers will be imposed, as well as measures to monitor the implementation of these measures through documents or audits.

Illustrative examples

Austria	*In the Telecom Network Security Regulation ("TNSR") available under: https://www.ris.bka.gv.at/eli/bgbl/II/2020/301, MNOs operating a 5G network will have to comply with information security measures and will have to maintain an Information Security Management System (ISMS) according to ISO/IEC 27 001 et al,*

[10] BEREC Internal survey prepared as input for the preparation of the EU Toolbox on 5G Cybersecurity.

certain 3GPP standards and further requirements. In addition, MNOs will be obliged to report 5G network functions and suppliers biannually to the NRA.

2.1.3 SM03 - Restrictions for high-risk suppliers

- Establish a framework with clear criteria, taking into account the risk factors identified in paragraph 2.37 of the EU coordinated risk assessment and adding country-specific information (e.g. threat assessment from national security services, etc.), for national competent authorities and MNOs to:

- Perform rigorous assessments of the risk profile of all relevant suppliers at national level and/or EU level (for example jointly with other Member States or other MNOs);

-Based on the risk profile assessment, apply restrictions- including necessary exclusions to effectively mitigate risks- for key assets defined as critical or sensitive in the EU coordinated risk assessment report (e.g. core network functions, network management and orchestration functions, and access network functions);.

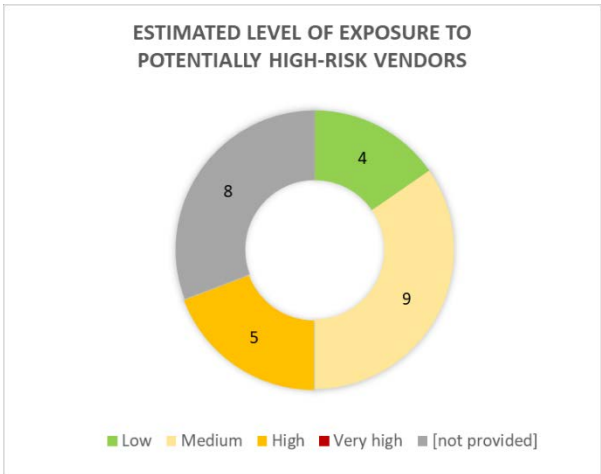
- Take steps to ensure that MNOs have adequate controls and processes in place to manage potential residual risks, such as regular supply chain audits and risk assessments, robust risk management, and/or specific requirements for suppliers based on their risk profile.

Estimated level of exposure to potentially high risk suppliers and existing mitigation

A majority of Member States who provided information on this point evaluate their level of exposure to potentially high-risk suppliers as **MEDIUM or HIGH** (fourteen Member States), while only three Member States consider their exposure to be currently low. For the others, no answer was provided or the information was considered too sensitive to be shared. Among them, several Member States noted that they currently do not have a framework in place for determining the risk profile of individual suppliers.

The main risks identified in the EU Risk assessment that are meant to be addressed by Strategic measures 03 and 04 are Risk 2 (lack of access controls) and Risk 5 (State interference through the 5G supply chain). These risks have both been rated as high or very high priority by a very large majority of Member States and as medium priority by a few others.

At the same time, a majority of Member States answered that medium to highly effective measures were already in place to mitigate Risk 2 (access controls). By contrast, for Risk 5 (risk of state interference), most Member States consider existing mitigation measures as insufficient.

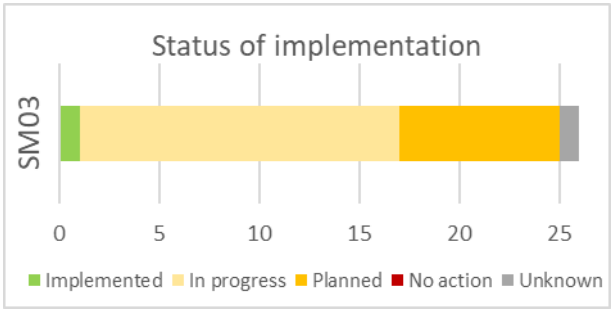


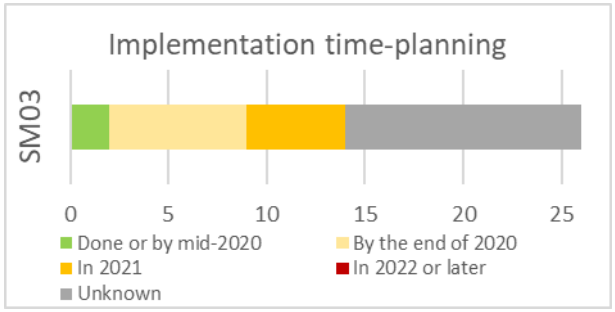
Status of implementation – statistics

The information received shows that this measure currently has a **MEDIUM** level of maturity. A few Member States have already implemented measures aimed at minimising the exposure to risks from suppliers considered to be high risk while in a large majority of other Member States, this process is

ongoing and in many cases well advanced. A small minority of Member States have not communicated specific information regarding their plans to implement this measure.

However, for those where a process has not been launched or completed yet, there is often also no clear information about the timeframe for introducing this measure. This might be related to the complexity and sensitivity of this measure, which requires taking into account a broader range of factors, in particular non-technical factors (e.g. risk of interference by a third country) as well as potential sector-specific costs and broader economic or societal impacts.





Status of implementation – details

The main determinants for the effective implementation of this strategic measure are:

a) the methodology used to assess the risk profile of suppliers, which should also take into account the criteria set out in the EU coordinated risk assessment[11], including non-technical factors;

b) the definition of key assets on which restrictions will apply; this should also be based on the categorisation of sensitive assets in the EU coordinated risk assessment and in particular take into account the fact that '*enhanced functionality at the edge of the network and a less centralised architecture than in previous generations of mobile networks means that some functions of the core networks may be integrated in other parts of the networks making the corresponding equipment more sensitive (e.g. base stations or MANO functions*)[12]';

A number of Member States indicate that restrictions in place or under development are based on specific risk assessments and on national security considerations. Based on available information, although there are variations in individual measures, the following has been shown about the approaches adopted or under consideration:

[11] The EU coordinated risk assessment report identifies several risk factors for the assessment of a supplier's risk profile, notably: the likelihood of the supplier being subject to interference from a non-EU country (this may be facilitated by, but not limited to, the presence of certain factors, which are also listed in the EU coordinated risk assessment report); the supplier's ability to assure supply; and the overall quality of products and cybersecurity practices of the supplier, including the degree of control over its own supply chain and whether adequate prioritisation is given to security practices.

[12] Conclusion of the EU Coordinated Risk assessment on 5G Cybersecurity.

- Pre-authorisation or notification/veto approaches: Assessing operators' plans and imposing restrictions or exclusions on a case-by-case basis, taking into consideration a variety of aspects, including the characteristics of individual suppliers as well as specific deployment modalities; this approach usually does not involve systematic or blanket supplier-specific measures;
- 'Deny list' approaches: Designating certain suppliers as high risk or untrusted and on this basis, applying restrictions or bans for operators to source certain equipment or services from them; restrictions under consideration may take the form of exclusions and/or caps on the share of the supplier(s) in the networks;
- 'Allow list' approaches: Identifying specific suppliers that would be allowed to supply 5G network equipment or services.

As regards the methodology and factors for assessing the risk profile of suppliers, at this stage, fourteen Member States have confirmed that their national framework includes or is expected to include non-technical factors (in some cases alongside technical factors), as identified in the EU coordinated risk assessment. Specific factors mentioned include objective factors such as the origin of suppliers or the risk of interference from third countries (e.g. taking into account the legal and political system of the third country). In addition, some Member States indicated that they are or will take into account country-specific information and/or threat intelligence. However, no specific information has been communicated regarding how the criterion of '*ability to supply'* will be taken into account. A few Member States suggested exploring the possibility of joint or EU-level risk profile assessments.

Regarding the identification of key network assets requiring higher protection, as of today, only one Member State has published a list of assets subject to pre-authorisation, which extends the scope of the regulatory powers beyond core network functions to cover also other highly sensitive parts of the networks (e.g. radio access network), in line with the Toolbox. A few others have announced that they would follow the Toolbox guidance as regards the rating of network asset sensitivity. These lists are still under elaboration and in some cases are not intended to be made publicly available. Another approach that has been mentioned consists of identifying all 5G elements and functions as sensitive and applying restrictions to the infrastructure as a whole.

As regards other types of key assets (geographical areas, critical infrastructures, government entities etc.), some Member States mentioned considerations related to the type of use cases and customer served. However, no further details about the identification of specific assets have been communicated for the purpose of this report.

Overall, on this last point (definition of key assets subject to restrictions), there is currently not enough information available to determine whether national approaches are converging to a sufficient extent and whether they will therefore result in effective mitigation of suppliers-related cybersecurity risks and avoid dependencies on high-risk suppliers as per SM05 and 06, which are closely related to the implementation of SM03.

Finally, it was noted that other infrastructure components critical to public electronic communications network such as fibre backbone infrastructure, may also be supplied by potentially high risk suppliers and therefore worth considering, possibly as part of the next phase in the EU coordinated approach.

Other relevant findings

In defining and applying these measures, the main other factors and considerations raised are similar as for SM01. They include the need to dedicate adequate resources to regulatory authorities, the relevance of potential sector-specific costs, which will depend on the degree of intervention and potential impact on contractual relationships, the timeframe for implementing measures and other factors related to the specific situation of individual operators. These potential costs should however be looked at also together with broader impacts in terms of business and societal resilience, also perceived as relevant or highly relevant in this context.

Illustrative examples

France	*Key network assets are defined in the Order of 6 December 2019 and regulated as sensitive assets subject to control and authorisation before being rolled out. Those key assets include the radio access functions and most core network functions.*
Italy	*Under the Golden Power law, the Government receives notifications concerning the use of equipment or services by MNOs for deploying 5G whenever this equipment or service is sourced from extra-EU suppliers. An inter-ministerial Coordination Group advises the Government about the opportunity of vetoing the contract (based on technical analysis) or imposing security measures.*
The Netherlands	*The Decree on safety and integrity of telecommunications of 28 November 2019 provides that untrusted suppliers will be designated on the basis of various criteria, including:* *(i) does the party that provides the service or product come from, or is under control of a party from, a country with legislation obliging commercial or private parties to cooperate with the government of that country, in particular with state organs charged with an intelligence or military task, or is the party a state-owned company?* *(ii) does the party that provides the service or product come from a country with an active offensive intelligence program aimed at the Netherlands and Dutch interests, or does the party come from a country with which the relationship may be strained to a degree that actions that may affect Dutch interests are conceivable.*

2.1.4 SM04 - Controlling the use of MSPs and equipment suppliers' 3rd line support

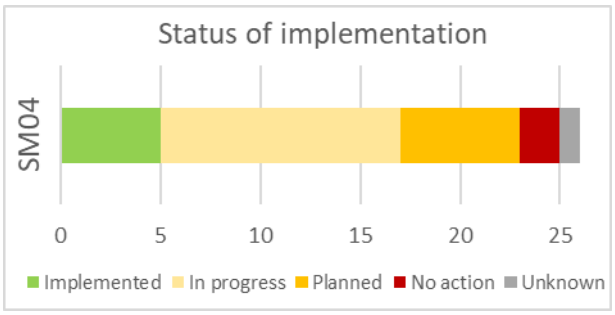
Establish a legal/regulatory framework which places limit on the types of activity and conditions under which MNOs are able to outsource particular functions to Managed Service Providers (MSPs), for both physical and virtual infrastructure, including:

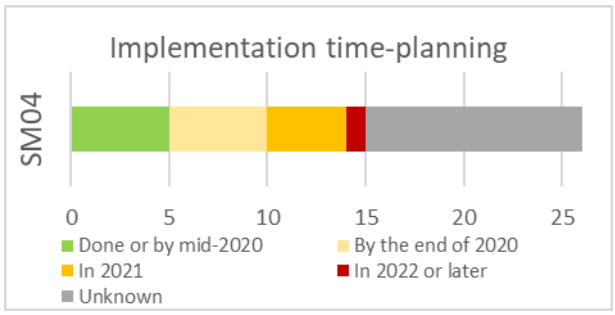
- Applying restrictions in particular in sensitive parts of the 5G networks, such as the security and network operations functions and where MSPs are considered to be high risk suppliers within the meaning of SM03;

- For functions outsourced to MSPs, impose enhanced security provisions around the access that MSPs are given to perform those functions.

Status of implementation – statistics

The information received shows that this measure currently has a **MEDIUM** level of maturity. While a majority of Member States have confirmed that measures are in place or underway, there is still little visibility of the extent to which detailed measures will address the potential outsourcing of important functions.





Status of implementation – details

A few Member States confirmed that they currently have a legal framework in place allowing them to fully implement SM04, including the possibility to restrict outsourcing or the use of specific Managed Service Providers considered to be high risk. On the latter (restriction to the use of high risk Managed Service Providers), the implementation of this measure is closely linked to the implementation of Strategic measure 03.

Several other Member States are currently in the process of preparing or considering measures that would provide such legal basis and set out possible limitations in this area, in line with the description of the Toolbox measure.

Moreover, some Member States report that certain operational and/or technical requirements applicable to the telecoms supply chain are in place or will be introduced, in order to mitigate security risks related to the outsourcing of certain functions, in particular as regards access controls.

A few Member States have not communicated clear plans to regulate the usage of MSPs.

Illustrative examples

Cyprus	*Forthcoming regulatory framework shall introduce limits on the types of activity and conditions under which MNOs are able to outsource particular functions to Managed Service Providers for both physical and virtual infrastructures. This includes sensitive elements of the 5G networks, enhanced security provisions regarding outsourcing and MSP remote access as well as strict access controls related to third line support.*
Finland	*MNOs are required ensure that, in a state of emergency, critical systems and their guidance, maintenance and control can be returned to Finland without delay. Traficom also has the power to issue regulations relating to network management.*

France	*To obtain an authorisation, an MNO must provide information regarding the operational modalities, specifying the configuration, supervision and maintenance operation likely to take place during the functioning of the equipment or on hosting services, as well as the list of contractors involved in operations, administration, maintenance and provisioning (OAM&P). In addition access control is also a key point of the technical assessment of the authorisation process.*
Ireland	*The Telecoms Security Requirements (TSRs) currently under preparation contain requirements which ensure the use of MSPs or vendor third line support does not adversely affect the overall security of the network. The TSRs define a number of technical and organisational controls that operators must implement to protect their networks from risks associated with third party access. The TSRs also contain requirements which ensure operators can flow down and enforce security measures to their suppliers through contractual arrangements.*

2.1.5 SM05 - Ensuring the diversity of suppliers for individual MNOs through appropriate multi-vendor strategies and avoiding dependency on high risk suppliers

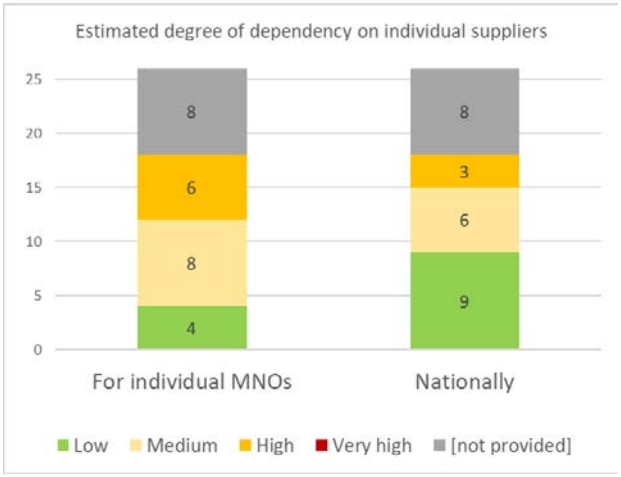
Ensure that each MNO has an appropriate multi-vendor strategy taking into account the technical constraints and interoperability requirements of the different parts of a 5G network:
- To avoid or limit any major dependency on a single supplier (or suppliers with a similar risk profile);
- To avoid dependency on suppliers considered to be high risk within the meaning of SM03.

Estimated level of dependency and existing mitigation

The current estimated degree of dependency for individual MNOs is high is six countries and medium in eight (eight Member States did not respond) while three Member States mention that there is a high degree of dependency on individual suppliers nationally, and six rate it as medium dependency.

It can be worth noting that among the five Member States that have indicated a high level of exposure to a potentially high risk vendor, in most cases also have stated that they have a high degree of dependency for an individual MNO and/or nationally.

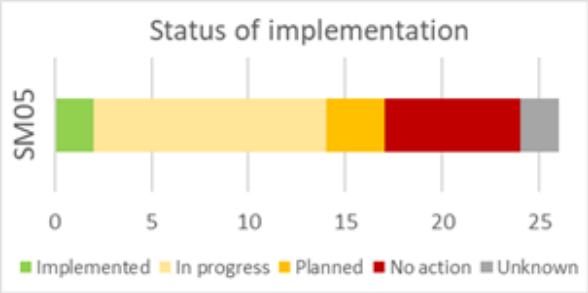
About half of the Member States believe that Risk 4 has very high, or high relevance and a majority of respondents answers that there are no, or only moderately effective means to mitigate the existing risk. This also correlates to the responses for Risk 5, linked to SM03 and SM04 as mentioned in previous sections.

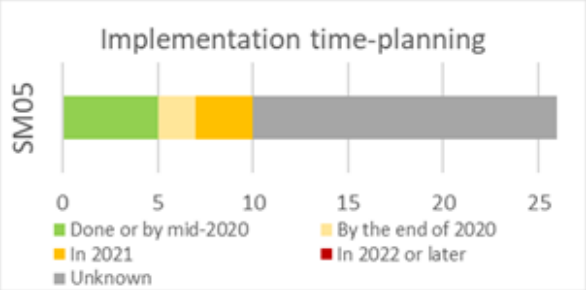


Status of implementation – statistics

This measure shows a **LOW** level of maturity. Indeed most Member States seems to be in the early stages of implementation of SM05 with about half of the respondents indicating that they have, or are in the progress of implementing measures but a majority have not indicated a time-plan of the implementation. Only two Member States have responded that they already have implemented measures addressing SM05 and ensuring that there is no major dependency on a single provider. Seven Member States indicated that they have not taken any actions and two Member States have not responded to questionnaire regarding SM05.

12 Member States have work in progress and five of them indicated that the measures will be implemented by the end of 2020. 16 Member States have not given any indication on when any measures will be implemented for SM05.





The answers do not allow to establish clearly if the implementation of the two different strands of SM05 (1. To avoid or limit any major dependency on a single supplier or suppliers with a similar risk profile and 2. To avoid dependency on suppliers considered to be high risk within the meaning of SM03) are dealt with in joint efforts or are handled separately.

As regards Strand 1 '**avoiding or limiting any major dependency on a single supplier'**, there are several ongoing national initiatives to further investigate the possible implementation of multi-vendor strategies even if not all Member States have started yet. Many Member States mention that it is not possible to mandate a multi-vendor strategy under their existing legislation so legislative changes are needed. Two Member States have seen a voluntarily implementation of multi-vendor strategies by MNOs.

Some Member States assess that SM05 is dependent upon the introduction of the new legislation transposing the Electronic Communications Code[13], while others consider linking it to the cybersecurity legislation. Further analysis is needed in many Member States to identify the appropriate legal basis to impose obligations in terms of diversification of suppliers.

As regards **'avoiding dependency on suppliers considered to be high risk within the meaning of SM03'**, some Member States are addressing this objective as part of the implementation of SM03

[13] Directive 2018/1972 of 11 December, 2018 establishing the European Electronic Communications Code (EECC). The EECC will replace the current European Telecommunications framework as of 21 December 2020.

(restrictions on high risk suppliers) in particular where Member States include in the list of assets to be protected a sufficiently large part of the network, so as to achieve a decrease in the dependency across the whole network.

Considerations raised by Member States related to potential implementation challenges include:

- The need to further define the exact scope and objective of "appropriate multi-vendor strategies", taking into account operator-specific and country-specific parameters;
- The need to assess existing dependencies, which requires having sufficient knowledge about the degree of involvement of suppliers in the various parts of the network, both in terms of existing market shares but also in terms of investment trends to ensure that there is a diversity of suppliers in the network rather than a major dependency in some legacy parts of the network and none in other parts;
- The relevance of the risk profile of the suppliers in assessing the dependency risk and defining appropriate mitigation;
- The existence of certain technical and operational difficulties to implement multi-vendor approaches in certain parts of the network; this requires addressing the underlying issue of (lack of) interoperability of equipment, as is also mentioned in the Toolbox, to avoid any situations of lock-in with a single supplier. Work will be carried out on this point within the NIS WS subgroup on standardisation (Supporting Action 03);
- Possible economic impacts on operators in case of strict diversification requirements, which also depends on the initial dependency level and on the timeframe for imposing potential changes;
- Possible increased difficulties for smaller Member States (difficulty to impose diversification within individual radio access network which increases the importance of diversification at national level and avoiding dependency on high risk suppliers);
- The current 5G supply chain market structure, with a limited number of alternative suppliers; and the need a coordinated EU effort driven by the European Commission to ensure a sustainable and sovereign EU supply chain (Strategic measure 07 and 08);
- Further EU-level coordination would be useful, including from the forthcoming input from BEREC.

Illustrative examples

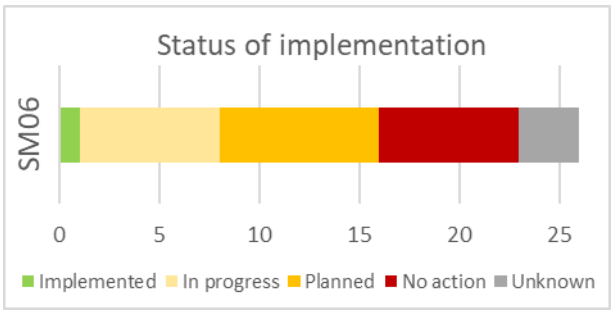
N.B: Examples relate only to 'Strand 1- diversification of suppliers'	
Cyprus	*The forthcoming regulatory framework will include guidelines for MNOs to develop and adopt appropriate multi-vendor strategies, using a risk-based approach. In general, this measure will take into account the need to keep additional burdens on MNOs limited to the minimum necessary, whilst ensuring appropriate levels of security and resilience.*
Italy	*Within the application of Golden Power to contracts related to core components, MNOs have been required to produce a diversification project including both "vertical" diversification (the use of systems from different suppliers in the hardware, virtualization and application layers) and "horizontal" diversification (the use of different software solutions, at application layer).*

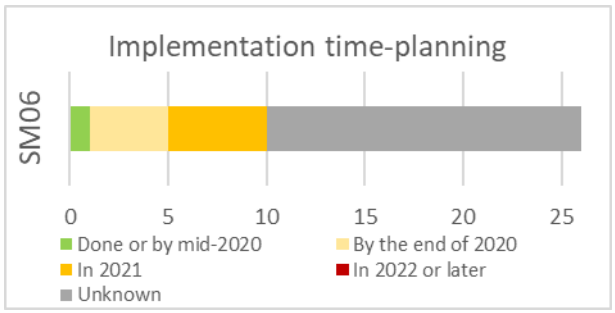
2.1.6. SM06 - Strengthening the resilience at national level

Ensure that there is an adequate balance of suppliers at national level to ensure that there is resilience in case there is an incident with one operator and/or one supplier, taking into account the variations in geography and population in individual Member States.

Status of implementation – statistics

The implementation of SM06 is currently at a **LOW** level of maturity. It is the least implemented strategic measure in the Toolbox according to the answers received. Only one Member States has implemented legal obligations regarding SM06 and seven Member States say that implementation is in progress. Ten Member States have answered that they have not taken any actions or not provided any answer. In terms of timeframe, five Member States have indicated that measures will be introduced before the end of 2020 while sixteen Member States have not given any indication on when or if any measures will be implemented for SM06 (with three Member States not responding to the question).





Status of implementation – details

Similarly to SM05 some Member States assess that the implementation of this measure is dependent upon the introduction of the new European Electronic Communications Code. A few Member States indicated that there is a wish for an EU wide approach and also for linking it to the activities of ENISA and BEREC. Several Member States replied that they are considering different options without giving further details.

Some Member States indicate that there are no active measures or implementation plans are in place since they currently assess that a national dependency does not exist (e.g. because there is currently an adequate balance of suppliers across national networks). However, where this is the case, some Member States note that they will monitor the evolution of the situation and could take action in the case of a risk of a decrease in diversity.

One concrete example provided of appropriate national diversification is given by a Member State where no single supplier represents more than 40 % of given market segment, except for some specific core network functions where the supplier is not considered as high risk.

Some Member States, mainly smaller countries, mention a risk of impact on competition between suppliers as well as potential increase of costs for operators.

Illustrative examples

Spain		Diversification objectives at national level will be considered in the national 5G Strategy.
Croatia		Measures to ensure resilience at national level through an adequate balance of suppliers are under consideration to be included in relevant legal acts.

2.1.7. SM07 - Screening of Foreign Direct Investment

Build on the EU's Foreign Direct Investment screening mechanism to improve the monitoring of FDI investments across the 5G value chain (e.g. through a mapping of key 5G assets, the use of monitoring tools and exploring specific guidelines), in order to better detect foreign investments in the 5G value chain that may pose a threat to the security or public order of more than one EU MS. Critical infrastructure, public security, access to and control of information and cybersecurity are well embedded under the scope of this (FDI) Regulation, allowing the evaluation of investments taking into account factors such as the risk profile of buyers/companies.

Status of implementation – statistics

Compared to the risks associated with this measure, the information provided by Member States shows that SM07 implementation remains at a **LOW-MEDIUM** maturity level. This relates both to the integration of Toolbox measures into existing screening mechanisms, as well as to the initial set up of such mechanisms themselves at national level.

National screening mechanisms are complemented by the EU level FDI screening Regulation due to be applied in October 2020. In this context, there are 14 EU Member States which have national screening mechanisms in place. Some of those mechanisms have been reviewed recently in anticipation of the full application of the Regulation, and several other Member States are looking into the adoption of screening mechanisms.

As regards the integration of the Toolbox measures into national FDI frameworks, it is too early to assess if Toolbox considerations are adequately covered by national screening mechanisms being planned, in progress or implemented at this point in time. In some cases, it seems that there are still implementation gaps such as legislation not covering the entire value chain or progress in legislation being dependent on progress in other Toolbox areas such as the more precise definition of assets. In other cases Member States are coordinating their legislative plans with the EU-level FDI screening Regulation ((EU)2019/452) application timetable.

Status of implementation – details

The aim of the questionnaire in this area is to assess if, when and how EU Member States are adapting or introducing national legislation on FDI screening mechanisms in order to take into account the 5G network value chain, and hence implement a prioritised mitigating measure of the Toolbox. Member States identified strengthened FDI screening mechanisms as a key measure in mitigating against the risk of single supplier dependency, and as an essential tool to identify key assets and foster a diverse and sustainable 5G ecosystem in the EU. Despite some gaps, the EU has an overall favourable position within the current 5G value chain. Yet, this position is not a given.

Changes in ownership due to FDI movements along this value chain have the potential of exposing 5G network value chains to higher cybersecurity risks overnight. The exposure to mergers and acquisitions seems especially high in times of economic challenges such as the ones caused by Covid-19, and adds to the urgency of the effective implementation of this point of the Toolbox.[14]

Based on the overall feedback to the questionnaire, the relevance of ownership and origin/establishment of suppliers of 5G equipment and services has been emphasised by many Member States. Moreover, as regards the impact of a potential major FDI in this area, one Member State commented that changes in ownership of suppliers through mergers and acquisitions could impact the exposure to risks drastically. The inclusion of FDI measures in the Toolbox therefore provides a further incentive to put into place new or strengthen already existing FDI screening mechanisms in Member States.

With the focus on FDI screening as strategic measure (SM07), the Toolbox targets investment by a foreign investor aiming to establish or to maintain lasting and direct links between the foreign investor and the target company in order to carry out an economic activity in a Member State. Typically, this can include both greenfield investments involving the creation of a new company or the establishment of facilities abroad, as well as transferring the ownership of existing assets to an owner abroad through mergers and acquisitions.

2.2 Stronger security requirements for mobile network operators

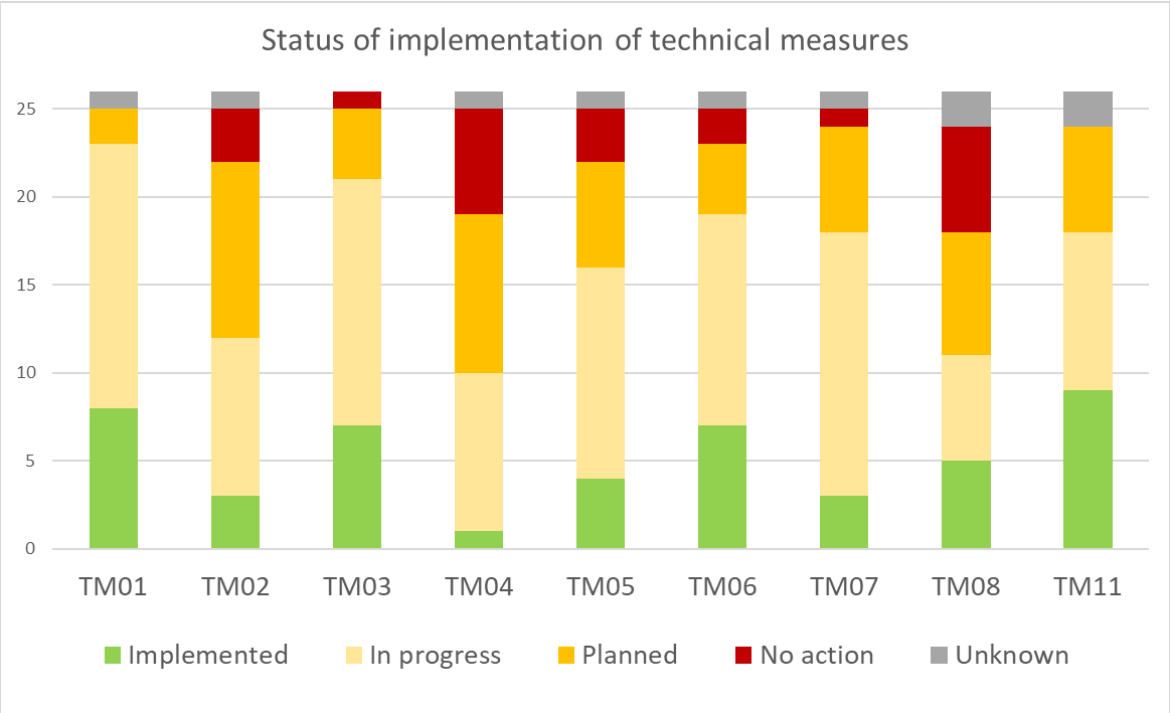
These measures from the Toolbox are related to strengthening of security requirements for MNOs, through the implementation of technical measures as listed in the Toolbox[15]. In this section we give an overview of findings related to implementation progress for each of the nine technical measures (TM01-TM08 and TM11).

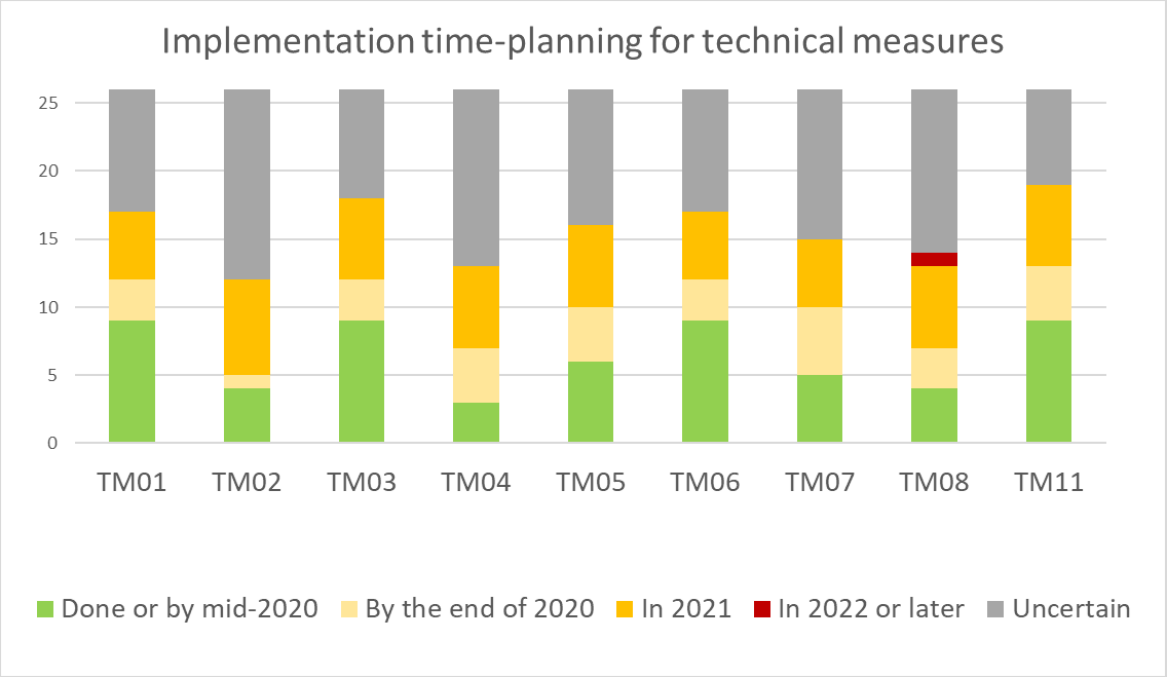
General findings

Overview

Looking at the current status of implementation of these measures, it is evident than many Member States have already taken concrete steps to accomplish them by starting, if not already completing, the implementation process. At the same time, there are differences in the levels of implementation maturity for different types of individual technical measures. The overall level of maturity for these measures can therefore be assessed as **MEDIUM**.

[14] This urgency has also been addressed at EU level in the Commission Guidance to the Member States (C(2020)1981) concerning foreign direct investment and free movement of capital from third countries, and the protection of Europe's strategic assets, ahead of the application of the EU's FDI screening Regulation.
[15] With the exception of measures TM09 and TM10, related to development of certification schemes.





Some of the measures, such as TM01 (related to application of baseline security measures) and TM11 (related to resilience and continuity), and, to some extent, also TM03 (related to access controls) are considered to be reasonably mature. This is likely due to the stable and relatively advanced process of defining, implementing and supervising similar requirements in the telecom sector, primarily under the scope Article 13a of the Framework directive[16]. At the same time, however, this may potentially create a false sense of security if these existing measures are considered sufficient, potentially

[16] https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures.

hindering actual strengthening of requirements for MNOs as envisaged in The toolbox. An illustration for this is the measure TM11, for which only three out of nine MS who have declared it as "implemented" have expressed some intentions to revise or further strengthen it. For the remaining six Member States, the data provided does not include explicitly stated intention of reinforcing of this measure beyond what is currently in place.

This need for strengthening existing technical measures, at least for critical assets in 5G networks, also appears to be recognised by many Member States, who are either already working on implementing such reinforcements, by revising existing or developing new guidelines or relevant legal instruments, or are actively making plans to do so. One Member State that already has legal instruments in the current framework regarding the technical measures has also stressed the importance to be cautious with categorising these measures as being "implemented", given the fact that the process concerning setting technical measures is still ongoing and thus may consequently give rise to need for update of existing measures.

On the other hand, security measures that dive deeper into specific areas of relevance for 5G networks or that are more closely related to still developing and evolving technology, or to future Stand Alone deployment options[17], such as those for implementation of measures in existing 5G standards (TM02) or for increasing of security in NFV (TM04) currently have a lower level of implementation maturity.

Similar could also be stated for the measure TM08, related to standards in supplier's processes. For these technical measures, the number of Member States who have not taken any actions yet or were not able to provide any data on status of implementation is visibly higher.

In the next sections, we present more details and specific findings from the assessment of each of the underlying technical measures, based on the data provided by MS.

2.2.1 TM01 - Ensuring the application of baseline security requirements

Ensure that MNOs implement existing security best practices and recommendations non-specific to 5G networks on, for instance product development, configuration, day-to-day network management, incident management, security updates[18], for instance by imposing and reviewing risk assessment plans by MNOs. Ensure that MNOs keep up-to-date information on security policy, including operational information, as well as linked to change and incident management procedures for key network and information systems.

[17] Stand-alone 5G architectures.

[18] *These measures should be based on international or European standards or technical guidelines, for example the Article 13a expert group guidelines of minimum security measures (*https://resilience.enisa.europa.eu/article-13/guideline-for-minimum-security-measures/Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf*).*

Status of implementation – statistics

Analysis of data provided by Member States shows that this measure has a **MEDIUM-HIGH** level of implementation maturity. In a great majority of Member States this measure is either already implemented or is underway (twenty-three Member States). Looking at time-lines of expected completion dates, half of the Member States expect to have the measure implemented this no later than the end of 2020.

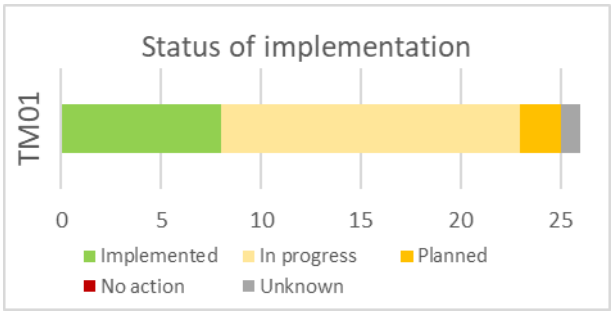
Status of implementation – details

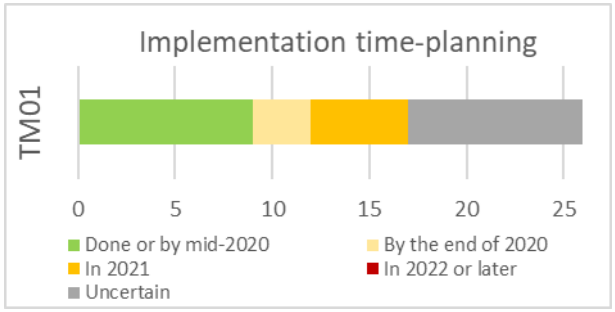
In many Member States, this measure is already implemented as part of the general security requirements for the telecom sector, under the current obligations, mostly on the basis of the Article 13a of the EU Framework Directive[19] and, in some cases, also based on specific obligations defined in national cybersecurity acts or other similar legislative instruments applicable to MNOs.

At the same time, many Member States have recognised and highlighted the importance of revising, enhancing, reinforcing or further security hardening of the existing baseline requirements. In many Member States the work on this is already underway, primarily in the scope of transposition of the European Electronic Communications Code or as part of development of other specific legal instruments for cybersecurity.

Some of the techniques and best practices recommended by Member States include:

- Segregation of trial network from the main core;
- Regular period security testing and vulnerability assessments by independent trusted third parties, including tests on backhaul protection systems;
- Design and manage 5G systems according to the recommendations released by the 5G-Ensure project[20], involving the company's security function.





Other relevant findings

Some Member States have also highlighted the link with Strategic Measures SM01 and SM02, stressing the importance of having appropriate regulatory powers, as to be able to enforce new or revised baseline security measures and to ensure their application by the means of conducting security audits of MNOs.

[19] To be succeeded by article 40 of the European Electronic Communications Code.
[20] https://www.5gensure.eu/.

Illustrative examples

Cyprus		*Most MNOs are certified with ISO27001 and maintain information security policies. Hardening procedures are followed based on suppliers/vendor recommendations and relevant best practices. However, this measure needs to be reinforced and expanded by the introduction of baselines to be followed by all operators and checked by the authority as part of the audit framework (SM02). In detail DSA[21] will consider including security hardening requirements at the application layer for operators and service providers following appropriate security guidelines.*

2.2.2 TM02 - Implementation of security measures in existing 5G standards

Ensure that MNOs and their suppliers implement the existing security measures in the relevant 5G technology standards (e.g. 3GPP) and use it as a minimum security baseline for MNOs, so as to ensure that also the optional parts of these standards, relevant for security, are adequately implemented.

Status of implementation – statistics

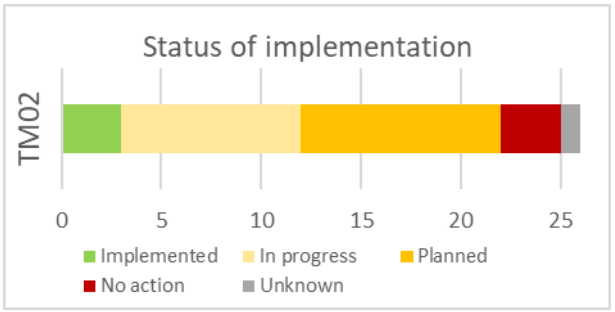
Analysis of data provided by Member States shows a **LOW-MEDIUM** level of implementation maturity. Only a minority (two Member States) consider it already implemented. In the remaining Member States, only a minority (nine Member States) reported that the implementation is underway. Looking at implementation timelines, there is an evidently high level of uncertainty regarding the concrete completion dates, as fourteen Member States have not specified any implementation date yet. The majority of the remaining Member States do not expect completion earlier than in 2021 (seven Member States).

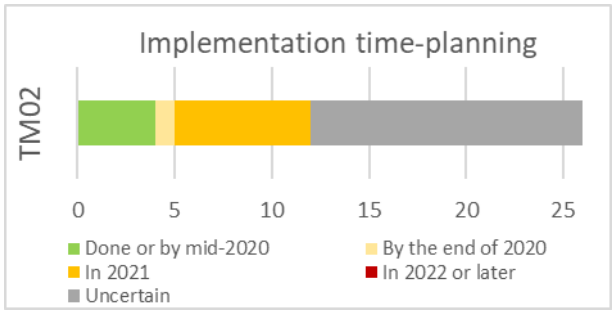
Status of implementation – details

While in some Member States, legislative instruments and relevant technical guidelines that are in place or that are currently being prepared include direct or indirect obligations for MNOs to comply with essential security requirements stemming from existing 5G standards (such as 3GPP), in other Member States these standards are not yet a point of reference to ensure security of 5G networks.

Some Member States have highlighted the fact that standards are still evolving and that their adoption and implementation by MNOs are still in early phase. Several Member States also underlined the importance of a coordinated EU-wide approach in this area and/or emphasized the importance of implementing related supporting actions from the Toolbox that could enable, support or increase effectiveness of the implementation of this technical measure. Some Member States intend to take further action once the work on the related supporting action SA04 advances and once further guidelines are provided by ENISA and the NIS Cooperation Group.

[21] Cyprus' Digital Security Authority.





Other relevant findings

Looking closer at the Member States input, it is indicative that incomplete data regarding the implementation dates is not caused by confidentiality concerns. This further affirms the difficulty of actual planning and estimating in the conditions of still evolving standards and network architectures and underscores the importance of stepping-up efforts for information and experience sharing and for coordinated EU-wide approach in addressing these issues.

Illustrative examples

Austria		*In the Telecom Network Security Regulation ("TNSR")[22], MNOs operating a 5G network will have to comply with essential 3GPP security standards. Implementation details: § 6 sect. 2 & Annex 1.*

2.2.3 TM03 - Ensuring strict access controls

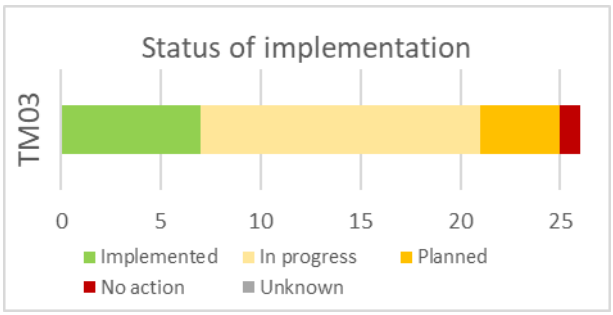
Ensure that MNOs implement adequate, flexible and verifiable technical measures to ensure that:
- Strict network access controls are applied;
- The principle of least privilege is applied, ensuring that various rights in the network (e.g. access rights between network functions, network administrators' rights, virtualisation configuration) are minimized;
- The segregation of duties principle is applied;
- Procedures are in place to ensure that these rules are in effect all the time and evolve with the network.
In setting the access control policies, particular care should be taken to ensure that remote access by third parties, especially suppliers considered to be high risk, is minimized and/or avoided whenever possible. When remote access is necessary, for example to address service outages, the MNO should apply appropriate authentication[23], authorization, logging and auditing so as to have a clear visibility on access to data and configuration changes or network alterations.

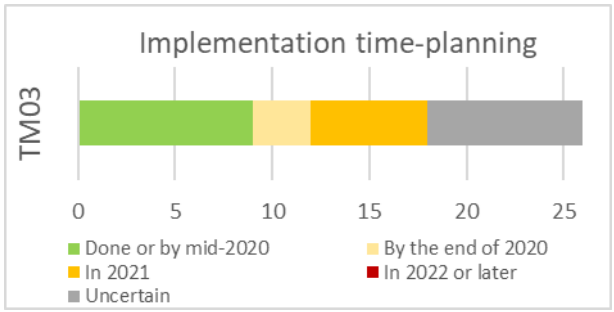
[22] https://www.ris.bka.gv.at/eli/bgbl/II/2020/301.

[23] In terms of authentication general good practices apply and appropriate mechanisms should be used, for example for temporary access by third parties and/or remote access (e.g. no permanent credentials, temporary (one-time) passwords, usable only for designated tasks should be used). These measures could, for example, be enforced by using appropriate Privileged Access Management (PAM) platforms.

Status of implementation – statistics

Analysis of data provided by Member States shows a **MEDIUM-HIGH** level of implementation maturity. In a majority of Member States, implementation is in progress (fourteen Member States). Only one Member States has indicated that there were no actions taken yet. Looking at time-lines of expected completion dates, a majority of Member States who have provided specific answers (six Member States) expects completion in 2021.





Status of implementation – details

Despite the fact that in number of Member States this measure is considered to be implemented already and that MNOs are considered to already have access control related measures implemented in line with relevant industry standards such as ISO 27001 or under the existing security requirements, there is an apparent need for further reinforcement of this measure, in line with the Toolbox recommendations and in relation to the underlying risks.

This need has been recognised by several Member States that stressed the importance of further strengthening of these measures for protection of critical parts of 5G networks and some are already working on implementing such updates.

In some Member States this technical measure is addressed through inclusion of related specific requirements in the authorisations required prior to the 5G auctions and in some Member States this measure is implemented as part of a relevant critical infrastructure security framework.

Some of the specific techniques and best practices recommended by Member States include:

- No remote support to Operation & Maintenance (outside the NOC);
- Remote access allowed in critical cases only, duly monitored;
- Access control to management applications (e.g. multi-factor authentication, centralised authorisation, authentication and access, privileged access management);
- Following of least privilege principle with access allocation and revocation processes in place
- Regular periodic (e.g. annual) access controls review;
- Controlling and monitoring of remote access – both for MNO employees and for third parties.

Illustrative examples

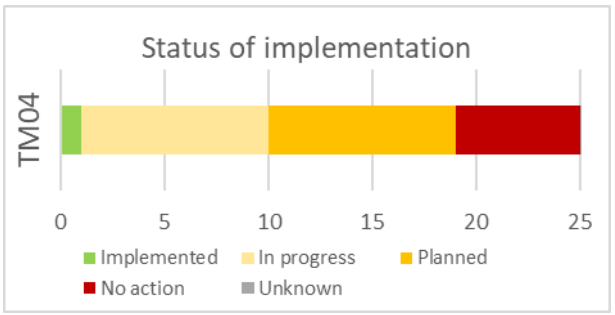
Ireland		*The TSRs contain detailed requirements for operators on Network Design and Access Control. This includes rules regarding network segmentation, access control and authorisation, multi-factor authentication (MFA), principles of least privilege and separation of duties. The TSRs also ensure operators implement appropriate logging and monitoring of access to detect anomalous activity.*

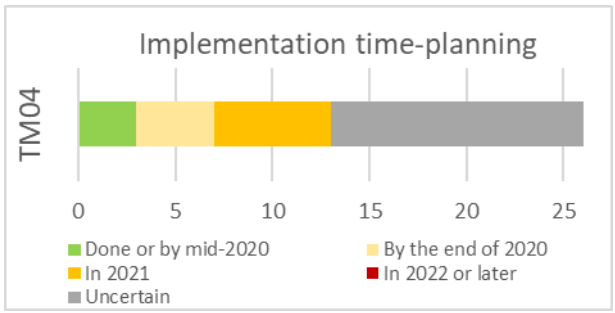
2.2.4 TM04 - Increasing the security of virtualised network functions

Ensure that MNOs follow security best practices for network function virtualisation. Note that there may be settings, for example when a network function is highly critical or when it is handling highly sensitive information, where virtualization is not appropriate and in such settings physical separation may be necessary.

Status of implementation – statistics

Based on the analysis of data provided by Member States, the maturity of this measure is assessed as **LOW-MEDIUM**. Only one Member State considers this measure as implemented and only in minority of the remaining Member States there is a reported progress in implementing this measure (nine Member States). Looking at implementation time-planning, there is a similarly high level of uncertainty regarding the concrete completion dates as it was the case for the TM02, as in half of the cases (thirteen Member States) there are no implementation dates specified. A majority of other Member States do not expect completion earlier than in 2021 (six MS).





Status of implementation – details

Information provided by Member States shows that best practices for security of network function virtualisation are yet to be identified and implemented. In some Member States explicit references to related security standards, such as ETSI NFV standards, are included and MNOs will have to comply with those standards.

Several Member States have also highlighted the fact that in the current phase of 5G development, virtualised networks have not yet been widely utilised and that the role of virtualization should be reviewed when 5G Stand-Alone architectures are deployed.

Activities planned to be undertaken by MS in order to implement this technical measure include:

- Hardening requirements to cover virtual networks;
- Periodical testing by independent professional and/or EU working groups;
- Improving the risk management process and taking-up of a risk-based approach on virtualisation;
- Including the related requirements in the authorisation process;
- Prescribing the state-of-the art for securing NFV;
- Working with private actors to improve risk management and the take-up of a risk-based approach on virtualisation.

Illustrative examples

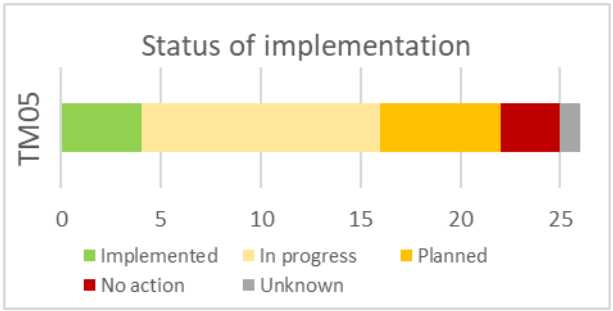
Examples from MS		
Austria		*In the Telecom Network Security Regulation ("TNSR")[24], MNOs operating a 5G network will have to comply with recommendations laid down in the ENISA document 'Security Aspects of Virtualisation'[25], February 2017. Implementation details: § 6 sect. 2 and Annex 1.*

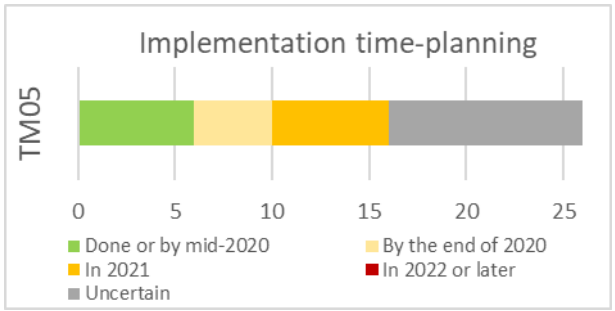
2.2.5 TM05 - Ensuring secure 5G network management, operation and monitoring

Ensure that MNOs run their Network Operation Centres (NOC) and/or Security Operation Centres (SOC) on premise, inside the country and/or inside the EU. The NOC and SOC are a vital component of the MNO's infrastructure in implementing and monitoring the measures for secure network management and operation. They should provide clear visibility and implement effective network monitoring of at least all the critical components and sensitive part of 5G networks, to detect anomalies and to identify and avoid threats, such as, for example, threats to the core network coming from compromised user devices and IoT).
Also ensure that MNOs appropriately protect the management traffic of the communications network or service to avoid unauthorised changes to the communications network or service components.

Status of implementation – statistics

Analysis of data provided by Member States shows a **MEDIUM** level of maturity. Only a minority (four Member States) considers the measure to be implemented already. In a majority of the remaining Member States the implementation is underway (twelve Member States). Looking at the implementation time-planning, there is a relatively high level of uncertainty regarding the concrete completion dates as high number of Member States have not specified any implementation date yet (ten Member States). The remaining Member States that are yet to complete the measure are split equally between those that expect completion to take place in 2020 (six Member States) and those where this is not expected earlier than 2021 (six Member States).





[24] https://www.ris.bka.gv.at/eli/bgbl/II/2020/301
[25] https://www.enisa.europa.eu/publications/security-aspects-of-virtualization

Status of implementation – details

In some Member States there are already requirements or practices in place related to the provisions of this technical measure, either as voluntarily implemented or as imposed on MNOs. Some Member States indicated the apparent trend among MNOs who currently run NOCs to deploy a SOC or to upgrade their NOC to provide SOC capabilities as well.

There is, however, an evident need for security hardening of related measures, in line with Toolbox requirements and new risks for 5G networks as identified in the coordinated EU risk assessment. Therefore, most Member States appear to be currently considering revising and reinforcement of these existing requirements or are already in the process of implementing such reinforcements. This typically includes identification of new obligations for MNOs, sometimes with explicit provisions for MNOs to operate 5G networks to ensure NOC/SOC operation on premises within EU territory and to have effective monitoring of all critical components and sensitive parts.

In some Member States this technical measure is addressed through inclusion of related requirements in the authorisations required prior to the 5G auctions and assignment of 5G pioneer spectrum bands.

Other ideas considered by Member States for implementation of this measure include:

- Request for MNOs to reach a high level of autonomy in running their network;
- Encouraging a cultural shift towards threat detection and incident response;
- Providing threat intelligence reports to MNOs and their extension to cover 5G networks;
- Defining interfaces between trusted and untrusted components and identifying possible solutions available to monitor these interfaces.

Other relevant findings

Some Member States have suggested reconsideration and possible extension of the limitations currently set in the Toolbox in relation to this measure in terms of *geography* (e.g. possible addition of EEA countries for operation of NOC/SOC) and of *scope* (expansion to covering other operations in addition to NOC and SOC).

Illustrative examples

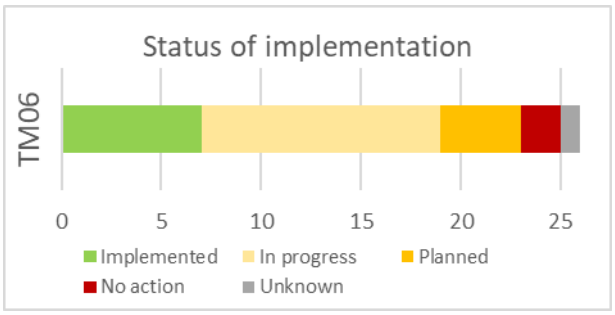
Examples from MS		
Italy		*Baseline requirements to address this technical measure are included in the Decree of Ministry of Economic Development "Security and integrity measures of electronic communication networks and notification of significant incidents" of the 12 December 2018 (secondary legislation), Article 4(1)(h) and (i).* *Within the application of the Golden Power, MNOs are not allowed to outsource the NOC and are requested to reach a high level of autonomy in running their networks*

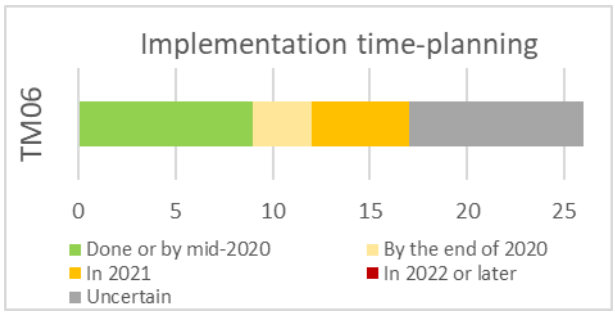
2.2.6 TM06 - Reinforcing physical security

Ensure that MNOs reinforce physical protection of critical components and sensitive parts of the 5G networks, taking a risk-based approach for Multi-access Edge Computing (MEC) and base stations[26], for example considering where the components are deployed and used, like a MEC use in hospitals. In reinforcing physical access controls, it is important to ensure that access is granted only to a limited number of security-vetted, trained and qualified personnel. Access by third-parties, contractors, and employees of suppliers/vendors, integrators, should be limited and monitored, particularly where it concerns critical components and sensitive parts of the 5G networks.

Status of implementation – statistics

Analysis of data provided by Member States shows a **MEDIUM** level of maturity for this measure. A significant majority of Member States has started, if not already completed the implementation of this measure (nineteen Member States). In only a very small minority of Member States there are no actions taken yet in relation to this measure (two Member States). Looking at time-lines of expected completion dates, out of ten Member States who have indicated expected completion dates, a half expects to have the implementation finalised by the end of 2020 and the remaining half in 2021.





[26] When doing the risk analysis, MNOs should consider the components and the service (like critical hospital MEC service).

Status of implementation – details

In many Member States it is typical that MNOs have their own security policies for accessing physical facilities, sometimes implemented under the current obligations for MNOs and/or as part of the critical infrastructure security frameworks. Many MNOs include all physical components in their risk assessments as well as BCP[27] and DRP[28]. Additionally, in many cases there are reportedly standard physical controls in place, such as CCTV, alarms, guards and fences where applicable deployed of protection of assets such as base stations and data rooms. However, physical controls on residential buildings are rare.

To address new risks specific to 5G network technologies, such as those related to Multi-Access Edge Computing (MEC), going a step further than traditional physical controls is both recommended in the Toolbox and further underlined in responses by Member States. In many Member States the process of revising and strengthening existing physical security guidance, primarily with the objective to ensure adequate mitigation of new risks specific to 5G, is underway. These initiatives are done either in the context of development of new guidelines and/or legislation, or as part of constant assessment of the effectiveness of existing measures and necessary adaptations following the progress and incorporation of new technologies

One of the potential challenges identified by some Member States is the apparent lack of full clarity at this moment on how MNOs will implement MEC, which may hinder the efforts to define specific and detailed security requirements in this area, at least on the short term.

Some Member States also highlighted the importance that other sectoral authorities receive adequate information to monitor the development of private 5G network within their sectors.

Illustrative examples

Examples from MS		
Austria		*According to the TNSR[29], MNOs operating a 5G network will explicitly have to ensure physical security of critical network components and sensible parts with regard to Multi-Access Edge Computing and base stations. Implementation details: § 6 sect. 3, subsection 4.*

2.2.7 TM07 - Reinforcing software integrity, update and patch management

Ensure that MNOs deploy adequate tools and processes to ensure software integrity, which reliably identify and keep track of changes and the status of patches, when performing software updates and applying security patches in the 5G networks.

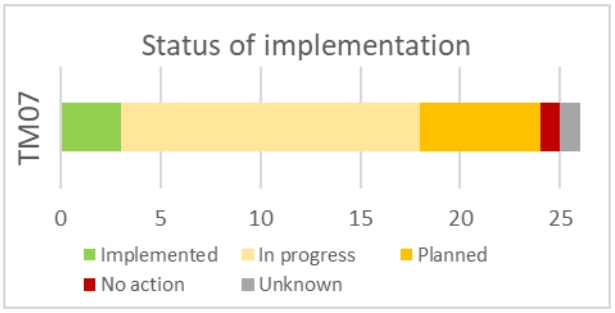
[27] Business Continuity Plans.

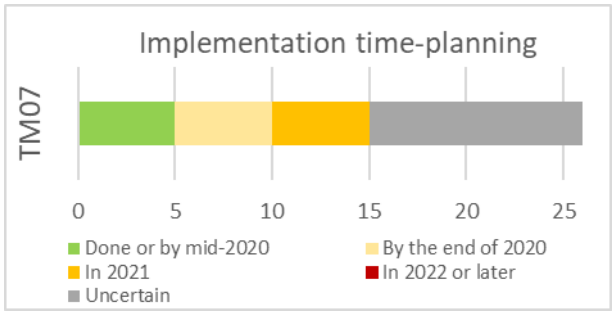
[28] Disaster Recovery Plans.

[29] https://www.ris.bka.gv.at/eli/bgbl/II/2020/301

Status of implementation – statistics

Analysis of data provided by Member States shows a **MEDIUM** level of maturity for this technical measure. In a majority of Member States the implementation is underway (fifteen Member States). Only a small minority considers this measure implemented (three Member States). Looking at implementation time-planning, there is a high level of uncertainty regarding the concrete completion dates as many Member States have not specified any implementation date yet (eleven Member States). In majority of the remaining Member States where the implementation is not yet completed (seven Member States) the expectation is that the completion will take place by the end of 2020.





Status of implementation – details

In a number of Member States there are existing patching policies and/or processes for software integrity, update and patch management in place, either as voluntarily implemented or as imposed on MNOs.

Many Member States are already considering hardening of these existing requirements or inclusion of additional specific obligations for MNOs, as to ensure adequate tools and processes in order to safeguard software integrity.

In some Member States this technical measure is addressed through inclusion of related requirements in the authorisations required prior to the 5G auctions.

Ideas considered by Member States for additional requirements include:

- Specifying requirements regarding the frequency and scope of MNO's patching process;
- Controlling or restricting automatic software updates;
- Testing of patches in lab environment and ensuring that devices are updated in controlled settings before deployments.

Illustrative examples

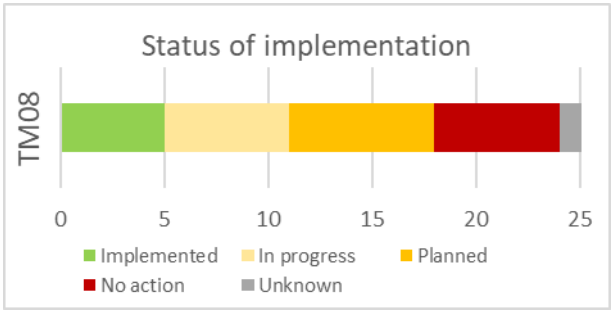
Examples from MS		
Netherlands		*The technical and organizational security requirements will be established in secondary legislation, as part of the Telecommunications Act. Obligations concern – among other things - access control, **security patching** and detection of incidents, network segmentation and third party software security.*

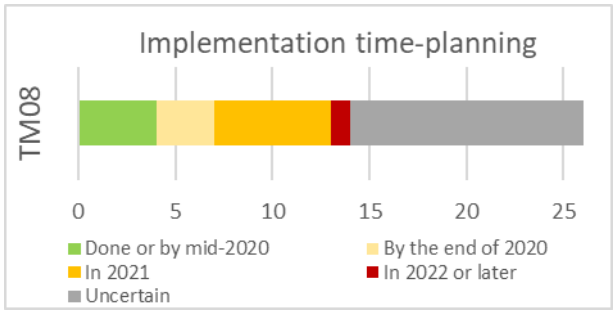
2.2.8 TM08 - Raising security standards in suppliers' processes through robust procurement conditions

Ensure that MNOs demand specific security standards from equipment suppliers in the procurement process (e.g. on specific security improvements and demonstrating quality levels, security maintenance of the equipment throughout its lifetime and built-in of security in the product' development processes).

Status of implementation – statistics

Analysis of data provided by Member States indicate high divergence in provided responses. In one half of the Member States the measure has either been fully or partially implemented or implementation is in progress (twelve Member States). On the other hand, there is relatively large number of Member States who have indicated that there were no actions taken yet (six Member States). Overall, the assessed level of maturity is considered **LOW-MEDIUM**. Looking at the implementation time-planning, there is an evidently high level of uncertainty regarding the concrete completion dates, as a significant amount of Member States have not specified any implementation date yet (twelve Member States). A majority of other Member States expect completion in 2021 or later (seven Member States).





Status of implementation – details

Even though suppliers are explicitly listed among relevant actors for this measure in the Toolbox, there is a general understanding among Member States that the ultimate responsibility for implementation of this measure lies with the MNOs. There is also a de-facto consensus among Member States that this could be achieved through robust procurement process. Such requirements, however, are not always part of the general security requirements for MNOs. Some Member States are now considering inclusion of such requirements, based on international best practices, including the ENISA *Baseline Security Requirements for procurement of secure ICT products*[30], while some are following EU measures in related legislation, such as the Radio Equipment Directive.

In some Member States, the approach to implement this measure is based on the system of authorisations for 5G deployments, applicable to both suppliers and MNOs, at least for the critical network assets.

[30] https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services/at_download/fullReport

Other relevant findings

Some Member States have also highlighted the link with Strategic Measures SM03 and SM04, vis-à-vis supplier risk assessment process as a way to reinforce existing requirements for procurement process.

Illustrative examples

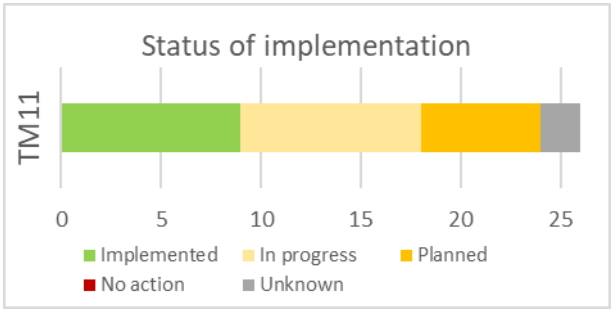
Ireland		*The TSRs include requirements for operators to include security requirements as part of their testing and evaluation process, including evaluating a suppliers' products lifecycle and security management. The TSRs also require operators to include clauses relating to product lifecycle & security management as part of their contractual arrangements with suppliers.*

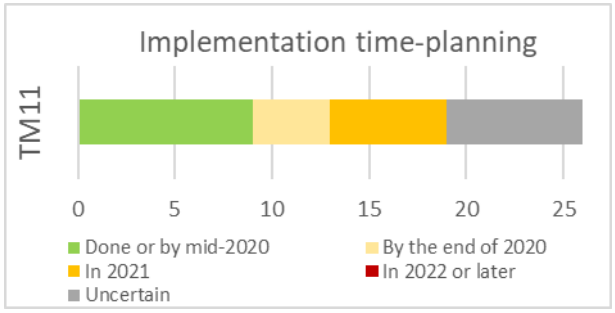
2.2.9 TM11 - Reinforcing resilience and continuity plans

Ensure that MNOs reinforce their resilience and continuity plans. MNOs should ensure they have adequate plans in place in case of disaster affecting the ongoing operation of their network, and ensure any critical dependencies are mapped and mitigated as required. MNOs should request similar arrangements within their suppliers and only use suppliers who demonstrate sufficient levels of long-term resilience.

Status of implementation – statistics

Analysis of data provided by Member States shows a **MEDIUM-HIGH** level of maturity for this technical measure. A majority of Member States (eighteen Member States) has either implemented the measure fully or partially (nine Member States) or has taken action to start the implementation process (nine Member States). Looking at time-lines of expected completion dates for Member States who are in the process of implementation, a majority of those Member States who have provided a response expect implementation completion in 2021 (six Member States).





Status of implementation – details

Looking further at the specific details provided by the Member States as regards the implementation of this technical measure, the predominant conclusion is that resilience measures are already in place, within the scope of current legal frameworks. On the other hand, however, six Member States who consider this measure to be implemented did not provide sufficient information to suggest that there is an intention to reinforce the measure, as suggested in the Toolbox (e.g. by mapping and mitigating of critical dependencies or by requesting MNO's obligations to demand resilience plans from suppliers). This indicates that there may be a false sense of security in some cases when it comes to the maturity of the implementation of this measure, based on the current requirements that are already in place which may hinder further reinforcement as envisaged by the Toolbox.

On the other hand, the need for further reinforcement of such measures in the context of securing 5G networks, as per the Toolbox requirements, has been implicitly or explicitly stressed by several Member States who consider the implementation of this measure to be in progress or is planned. In a number of cases, Member States indicated intention to further revise existing measures and to add complimentary or additional requirements.

In some Member States, the matter of resilience and continuity falls under the national security strategy domain. Some Member States also highlighted the importance of critical dependencies between 5G networks and other critical sectors.

Other relevant findings

Looking back at the underlying risks that this measure is expected to address - risk R7 (*significant disruption of critical infrastructure services*) and risk R8 (*massive failure due to power interruption*), it is indicative that a majority of Member States who responded to the question on the existence of effective mitigating measures consider to have reasonably or highly effective measures in place already (more than sixteen Member States). This is consistent with the overall indication of relative maturity of implementation of requirements envisaged under this technical measure.

Illustrative examples

Belgium		*Risk assessment are reported to NRA including security measures in place.* *In the context of the critical infrastructure (which will include 5G), NRA are monitoring the execution of regular continuity exercises by operators.* *A sectoral telecommunication crisis plan is maintained by NRA and periodic exercises are organised.*

3 Conclusions

This report analyses the progress made by Member States in implementing the measures recommended in the conclusions of the EU Toolbox on the cybersecurity of 5G networks, which was published on 29 January 2020.

All Member States reported that concrete steps have been taken to implement the Toolbox. Most Member States carried out a gap analysis and launched a process to review and upgrade existing

security measures and enforcement mechanisms. Many Member States have already adopted or are well advanced in the preparation of more advanced security measures on 5G cybersecurity.

However, work is still ongoing in many Member States on defining the content and scope of the measures and in some cases, political decisions still need to be made in this regard. In addition, even where measures are in progress or being planned, not all Member States have shared detailed information about every measure, due to diverse stages in the national implementation process or for national security reasons. Nevertheless, a number of findings can be formulated based on the analysis presented in this report as regards the implementation of the Toolbox and areas where specific attention is needed in the next phases of the implementation of the Toolbox at national and/or EU level.

Measure	Maturity	Findings and next steps
SM01 and (Strengthened powers for regulatory authorities)	MEDIUM/ HIGH	A large majority of Member States are in the process of significantly **strengthening national regulatory powers, including ensuring that authorities have powers to regulate the procurement of network equipment and services by operators**, based on security-related grounds. It is important that this process is completed as soon as possible.
SM02 (audits and information)	MEDIUM	While national regulatory authorities already have powers to conduct audits, there is currently not sufficient information to analyse whether Member States are planning to **perform more regular and detailed audits and to request more information from operators** about 5G equipment procurement and deployment plans. Further information-sharing on this measure would be helpful.
SM03 (Restrictions on suppliers based on their risk profile)	MEDIUM	In a large majority of Member States, the implementation of **measures aimed at minimising the exposure to high-risk suppliers**, based on clear criteria as defined in the EU Coordinated Risk Assessment and in the Toolbox[31], is ongoing and in many cases is well advanced. However, due to the complexity and sensitivity of the matter, in some Member States (one third of them approximately), there is still some uncertainty concerning the timeframe for adoption. It is important that this process is further advanced and completed in the coming months. When assessing a supplier's risk profile, as regards the criteria 'ability to assure supply' identified in the EU coordinated risk assessment, it is recommended that the assessment take into account the international trade context. When fully implementing this measure, **specific attention is needed as regards**: - Identifying key assets that are or will be subject to restrictions (including necessary exclusions) by looking at the network as a whole, and applying them to core network functions as well as to other key assets, including NFV management and orchestration (MANO) and the radio access network, in order

[31]The criteria listed include: the likelihood of the supplier being subject to interference from a non-EU country, the ability to assure supply and the overall quality of products and cybersecurity practices of the supplier. More details in paragraph 2.37 of the EU coordinated risk assessment.

		to address risks in a timely manner, as these assets will become critical or highly sensitive in 5G networks (in particular during the standalone phase of 5G deployment), as identified in the EU wide risk assessment and the Toolbox; - Imposing measures to protect also other types of key assets, such as defined geographical areas, government or other critical entities; - Defining implementation plans and/or transition periods for those operators currently using equipment of high-risk suppliers or having already entered into contracts with high-risk suppliers before the adoption of the Toolbox (e.g. by taking into account equipment upgrade cycles, in particular the migration from 'non stand-alone' to 'stand-alone' 5G networks).
SM04 (Controls on MSPs)	MEDIUM	A significant number of Member States appear to have yet to review existing practices and adopt **measures to limit the types of activity and conditions under which MNOs are able to outsource particular functions**, as per SM04 in the Toolbox. Where this is not yet the case, it is recommended to urgently consider measures in this area and to include them in national implementation plans.
SM05 and SM06 (Diversification of suppliers- for each operator and nationally- and avoiding dependency on high risk suppliers)	LOW	Most Member States have not yet established or communicated clear plans to effectively **address existing situations of dependency on high-risk suppliers and prevent future dependencies**. Avoiding such dependency is closely linked to the implementation of SM03 and to the scope of restrictions placed on high-risk suppliers, which should consider the network as a whole (i.e. restrictions applied to core network functions as well as to other key assets, including NFV management and orchestration (MANO) and the radio access network). Progress is urgently needed to mitigate this important risk, also with a view to reducing dependencies at Union level. This should be based on a thorough inventory of the networks' supply chain and implies monitoring the evolution of the situation. Many Member States are currently experiencing challenges in **designing and imposing appropriate multi-vendor strategies for individual MNOs or at national level**, which can be a complex process because of technical or operational difficulties (e.g. lack of interoperability, size of the country). Further work should therefore be done to clarify the parameters of 'appropriate multi-vendor strategies' under SM05, in particular through further exchanges of experiences and best practices within the NIS Work Stream and within BEREC. On this basis, Member States should also assess the need for additional measures to ensure national resilience.
SM07 (Supply chain resilience and EU capacities)	LOW-MEDIUM	The protection of strategic assets is seen as an essential underlying condition for ensuring the cybersecurity of 5G networks in the EU and meeting the objectives of the Toolbox. Several Member States have recently taken steps to **introduce or reinforce existing national FDI screening mechanisms**. Steps should

		be taken to introduce such mechanism without delay in 13 Member States where it is not yet in place, including in view of the approaching application of the EU screening framework as of October 2020. The screening mechanisms should be applied to investment developments potentially affecting the 5G value chain, taking into account the objectives of the Toolbox (SM07 and SM08).
Technical measures (strengthened security obligations on operators)	MEDIUM[32]	In a majority of Member States, there is an ongoing process of **reviewing and reinforcing network security requirements for operators** and in some Member States this process is well-advanced. However, few details about the content of some of the measures is available at this stage. It is important to ensure that network security and resilience requirements are strengthened, that they follow the latest state-of-the-art practices and that their implementation by operators is effectively audited and enforced. To support this process, it is also important that the new, updated guidelines on security measures for MNOs, including specific 5G-technology related aspects, are developed and agreed at the latest by the end of 2020, with the help of ENISA, in order to implement the toolbox supporting action SA01. Progress is slower when it comes to technical measures for mandating key security requirements from 5G standards or securing the NFV, as well as strengthening technical requirements for suppliers (e.g. through procurement). This is, in some cases, directly linked to the fact that 5G is by nature an evolving technology with some uncertainties on the way it will be implemented and deployed. To support implementation of some of these technical measures, it is also important that related supporting actions from the Toolbox are addressed, including: - the development of the new guidelines on security measures in existing standards (as per the supporting action SA04); - ensuring increased European engagement in relevant standardisation bodies and contributing to achieving an appropriate level of convergence as regards technical measures relying on standardisation and certification, in line with existing legislation, such as but not limited to the Cybersecurity Act (as per the supporting action SA03), including through the subgroup on standardisation and certification.
Other EU level actions		Going forward, to further support the Toolbox implementation and promote convergence between national approaches on the findings highlighted in this report, it is also recommended to: - Intensify efforts to **exchange information among Member States about the challenges, best practices and solutions** for implementing the Toolbox measures. through the use of

[32] Maturity for individual technical measures varies from [LOW-MEDIUM] to [MEDIUM-HIGH]. The average maturity across all technical measures is MEDIUM.

		existing information sharing mechanisms (as per The toolbox supporting action SA09); in particular, this should include further exchanges regarding the assessment of suppliers' risk profiles as per SA06 and as regards identifying key assets and imposing restrictions on them, for example when the same MNO is operating in more than one Member State; - Continue **monitoring and evaluating the implementation of the Toolbox**, with a view to informing the review of the March 2019 Commission Recommendation and identifying areas for possible measures at EU level, with the help of the Commission and ENISA; - Continue **working together with the Commission to further implement EU-level actions** listed in the toolbox. This includes actions aimed at: - Further strengthening EU capacities in the 5G and post-5G technologies, by using relevant EU programmes and funding (as per SM08); - Avoiding distortions in the 5G supply market stemming from potential dumping or subsidies; - Facilitating coordination between Member states regarding standardisation to achieve specific security objectives and developing relevant EU-wide certification scheme(s); and - Ensuring 5G projects supported with public funding take into account cybersecurity risks (as per SA10).